

Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 21, Issue 1

2011

Article 5

VOLUME XXI BOOK 1

The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed

Stephanie A. DeVos*

The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed

Stephanie A. DeVos*

| | |
|--------------------------------------------------------------------------------------------------------------------|-----|
| INTRODUCTION | 174 |
| I. BACKGROUND: CYBERSECURITY POLICY, GOOGLE, AND THE NSA | 178 |
| A. History of United States Cybersecurity Policy..... | 179 |
| 1. 1998–2002..... | 179 |
| 2. 2003–2008..... | 182 |
| 3. 2009–present..... | 187 |
| B. <i>The Google-NSA Alliance</i> | 190 |
| 1. Background Information: Google and the NSA .. | 190 |
| a) Google | 190 |
| b) The National Security Agency | 196 |
| 2. Events Prompting the Formation of the Google-NSA Alliance | 198 |
| II. IF GOOGLE IS APPROACHING THE NSA TO PROTECT ITSELF, ARE CURRENT GOVERNMENT POLICIES PROVING INEFFECTIVE? | 206 |
| A. The Google-NSA Alliance Is a Marked Departure from Current Policy and Demonstrative of its Ineffectiveness..... | 206 |
| 1. The NSA Is the Designated Government Agency | 206 |
| 2. Information Sharing: Problems, Questions, and Concerns | 209 |

| | |
|------|------------------------------------------------------------------------------------------------------------|
| 174 | <i>FORDHAM INTELL. PROP. MEDIA & ENT. L.J.</i> [Vol. 21:173] |
| 3. | The Alliance Is Answering a Call for Change..... 212 |
| 4. | The Government Is Not Keeping Pace with Its Plan 213 |
| B. | The Google-NSA Alliance Reflects the Effectiveness of Current Government Cybersecurity Policy 214 |
| 1. | The Alliance Can Be Characterized as a Public- Private Partnership..... 215 |
| 2. | The Alliance Was Formed Voluntarily 216 |
| 3. | The Alliance Represents a Step Toward Addressing Cyber Vulnerabilities and Best Practices..... 217 |
| 4. | The Alliance Promotes Information Sharing Between the Public and Private Sectors..... 218 |
| III. | PROBLEMS ACROSS SECTORS FURTHER SUGGEST THAT CURRENT CYBERSECURITY POLICY NEEDS IMPROVEMENT . 219 |
| | CONCLUSION..... 226 |

INTRODUCTION

Privacy rights have been a hotly debated issue for the past few decades, increasingly so with the ever-growing presence of the Internet in the daily lives of Americans. The reach of the Internet has expanded so significantly that according to a recent poll conducted by BBC World Service, nearly four out of five people across the world believe that access to the Internet is a fundamental right.¹ This survey of more than 27,000 adults across twenty-six countries suggests that the Internet should be regarded as basic infrastructure and that this right to communicate should not be ignored.² While some countries, including Finland and Estonia, have ruled that Internet access is a human right for their citizens, questions remain about the appropriate level of government oversight of certain aspects of the Internet.³ Though nearly seventy-nine percent of the survey respondents either strongly agreed or somewhat agreed with the characterization of access to

¹ *Internet Access Is ‘A Fundamental Right,’* BBC NEWS, Mar. 8, 2010, <http://news.bbc.co.uk/2/hi/8548190.stm>.

² *Id.*

³ *Id.*

the Internet as a fundamental right and believed in its positive impact in bringing them greater freedom, many also expressed concerns: in rank order, these included fear of fraud, easy access to explicit and violent content, and privacy worries.⁴

The fact that privacy appears third on this list of concerns is itself disturbing. Think about how much time you, the reader, spend on the Internet each day. You can read your e-mail messages, make a purchase online, read a blog,⁵ or conduct searches using Google,⁶ Bing,⁷ Yahoo!,⁸ or another of the myriad of Internet search engines available. Both the sheer number of users, each conducting individual activities on the Internet, and the amount of personal information shared in each of those activities (e.g., typing in an e-mail password, or entering a credit card number when making an online purchase) is staggering. If this highly sensitive information, or even something more innocuous such as a user's search terms,⁹ were to enter the wrong hands, the consequences could be dire.

In response, the United States government, beginning in 1998, created initiatives aimed at the protection of cyber systems. These initiatives designated cyber systems as a part of the nation's critical infrastructure.¹⁰ Subsequent government initiatives were designed to reinforce the important role of cyberspace in America, while striving to maintain a balance between government oversight and

⁴ *Id.*

⁵ See Michael Conniff, *Just What Is a Blog, Anyway?*, ONLINE JOURNALISM REV. (Sept. 29, 2005), <http://www.ojr.org/ojr/stories/050929>.

⁶ *Google Corporate Information, Company Overview*, GOOGLE, <http://www.google.com/corporate> (last visited May 2, 2010).

⁷ *Discover Bing*, BING, <http://www.discoveringbing.com/behindbing/about.aspx> (last visited May 2, 2010).

⁸ *Corporate Information*, YAHOO!, <http://info.yahoo.com/center/us/yahoo/> (last visited Aug. 10, 2010).

⁹ See, e.g., *About Google Trends*, GOOGLE TRENDS, <http://www.google.com/intl/en/trends/about.html> (last visited Sept. 13, 2010). Google Trends allows a user to see data about how often a given topic has been entered into the Google search engine over time, on a particular day, or in a specific geographic region. *Id.*

¹⁰ WHITE HOUSE, CRITICAL INFRASTRUCTURE PROTECTION PDD-63 1–2 (May 22, 1998) [hereinafter PDD-63], available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf>; see also *infra* Part I.A.

individual privacy rights.¹¹ Several prominent privacy rights organizations have heavily criticized the government's involvement in Internet regulation and security.¹²

The efforts of private corporations to protect personal data online have also been subjected to criticism. For example, the satirical newspaper *The Onion* recently published an article in response to some of the privacy concerns associated with the Internet giant, Google.¹³ While the article specifically attacked a new Google service that had recently launched,¹⁴ it also generally described a worst-case scenario involving the private data of Google users. It reported a fictitious apology issued by Google CEO, Eric Schmidt. In the article, Schmidt apologized to Google users, "particularly the 1,237,948 who take daily medication to combat anxiety—for causing unnecessary distress, and . . . expressed regret—particularly to Patricia Fort, a single mother taking care of Jordan, Sam, and Rebecca, ages 3, 7, and 9—for not doing more to ensure that private information remains private."¹⁵

¹¹ See, e.g., PDD-63, *supra* note 10.

¹² See, e.g., CTR. FOR DEMOCRACY & TECH., <http://www.cdt.org/issue/cybersecurity> (last visited Sept. 13, 2010); *Cybersecurity Privacy Practical Implications*, ELEC. PRIVACY INFO. CTR., <http://epic.org/privacy/cybersecurity/default.html> (last visited Sept. 13, 2010); *Online Privacy & Technology*, PRIVACY RIGHTS CLEARINGHOUSE, <http://www.privacyrights.org/Online-Privacy-and-Technology> (last visited Sept. 13 2010); *Technology and Liberty*, AM. CIVIL LIBERTIES UNION, <http://www.aclu.org/technology-and-liberty> (last visited Sept. 13 2010); *cf. U.S. DEP'T OF HOMELAND SEC., DHS PRIVACY OFFICE ANNUAL REPORT TO CONGRESS 44–45* (Sept. 2009), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf. Despite the vocal criticisms of government regulation of the Internet, only two pages of the most recent DHS privacy report to Congress are dedicated to cybersecurity. *See id.*

¹³ See *Google Responds to Privacy Concerns with Unsettlingly Specific Apology*, THE ONION (Mar. 2, 2010), http://www.theonion.com/content/news/google_responds_to_privacy [hereinafter *Google Responds to Privacy Concerns*].

¹⁴ *Id.* On February 9, 2010, Google launched a product called Buzz, which created a social networking platform within Gmail, Google's webmail service, through which users were set up to automatically "share" interesting items (photos, videos, links to Web sites, etc.) with the user's most frequent Gmail contacts. Several days later, Google made a number of improvements in response to a flurry of user criticisms concerning the privacy of their individual data as visible through Buzz. *See Todd Jackson, A New Buzz Start-Up Experience Based on Your Feedback*, OFFICIAL GMAIL BLOG (Feb. 13, 2010, 3:53 PM), <http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html>; Todd Jackson, *Introducing Google Buzz*, OFFICIAL GOOGLE BLOG (Feb. 9, 2010, 11:06 AM), <http://googleblog.blogspot.com/2010/02/introducing-google-buzz.html>.

¹⁵ *Google Responds to Privacy Concerns*, *supra* note 13.

The point of the article was to illustrate exactly how much personal information is available over the Internet, and especially to show the astounding amount of data shared within Google's individual services (e.g., search and e-mail). While the piece is clearly an exaggeration, it satirizes lingering Internet privacy concerns. Such concerns represent a significant part of the discussion regarding the recent alliance formed between Google and the National Security Agency. This alliance was formed in response to cyberattacks¹⁶ which originated in China and targeted Google's corporate infrastructure.¹⁷ As a consequence of these cyberattacks, some of Google's intellectual property was stolen, prompting it to enlist the assistance of the National Security Agency to improve the security of its digital infrastructure.¹⁸

This Note seeks to explore the alliance between Google and the National Security Agency and how it fits within the framework established by the government to protect the critical technology and cybersecurity infrastructure of the United States. It will address whether the alliance is consistent with or represents a departure from existing government policies, in terms of its effectiveness and the consequences for privacy protection. This Note argues that the alliance, while retaining certain elements of current government cybersecurity initiatives, points to clear deficiencies in these policies and answers several recent calls for change in cybersecurity programs. This Note concludes that while the Google-NSA alliance is a significant step toward improved cybersecurity, more work needs to be done in order to adequately protect cyberspace.

Part I will investigate the history of the United States cyberspace policy from the Clinton administration to the present administration. It will also explore both Google and the NSA as individual entities and outline the available details about the alliance. Part II will examine both sides of the debate regarding

¹⁶ See *What Is a Cyberattack?*, WISEGEEK, <http://www.wisegeek.com/what-is-a-cyberattack.htm> (last visited May 2, 2010) ("A cyberattack is an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission.").

¹⁷ See *infra* Part I.B.1.

¹⁸ See *id.*

whether the Google-NSA alliance is a product of existing cybersecurity policy or whether it highlights deficiencies in the existing regime. Finally, Part III of this Note will argue that the Google-NSA alliance retains the fundamental principles of present cyber policy initiatives, but the alliance's innovations point to deficiencies in existing U.S. cybersecurity policy which indicate that the current framework needs improvement. This Part will also discuss the cybersecurity deficiencies that exist within critical infrastructures of the defense sector, and conclude that problems across two critical infrastructure sectors suggest that government cybersecurity policies to date have been largely deficient and thus require improvement.

I. BACKGROUND: CYBERSECURITY POLICY, GOOGLE, AND THE NSA

President Barack Obama has identified cybersecurity as one of the most significant national security challenges faced by the United States today, and recently stated that the nation is not sufficiently prepared to respond to cyber threats.¹⁹ Nevertheless, there are initiatives currently in place for reviewing and improving our nation's cybersecurity,²⁰ all of which address the goal of protecting and securing the United States in cyberspace.²¹ In order to comprehend some of the current strategies to achieve this

¹⁹ NAT'L SEC. COUNCIL, THE COMPREHENSIVE NATIONAL SECURITY INITIATIVE 1 (Mar. 2, 2010), available at <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>.

²⁰ See, e.g., U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN (2006) [hereinafter 2006 NIPP], available at <http://www.fas.org/irp/agency/dhs/nipp.pdf>; WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009) [hereinafter CYBERSPACE POLICY REVIEW], available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003) [hereinafter NATIONAL STRATEGY TO SECURE CYBERSPACE], available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf; Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003) [hereinafter HSPD-7], available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtml#1; Press Release, White House, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2010) [hereinafter Remarks by the President], available at <http://www.whitehouse.gov/the-press-office/remarks-president-secluding-our-nations-cyber-infrastructure>.

²¹ THE COMPREHENSIVE NATIONAL SECURITY INITIATIVE, *supra* note 19.

2010]

CYBERSECURITY AT INTERNET SPEED

179

objective, one must have a broad understanding of past and present cyberspace policy, as well as background knowledge of the two organizations comprising the Google-NSA alliance.

A. History of United States Cybersecurity Policy

Citing the nation's increasing reliance on cyber-based information systems, the United States government began focusing on the cyber aspects of critical infrastructure in 1998.²² Since then, the nation's reliance on the Internet has increased exponentially and cybersecurity initiatives have reflected this augmented usage, focusing on several particular areas: partnerships between the public sector and private industry, information sharing in cyberspace, and concern for the privacy rights and civil liberties of the individual.

1. 1998–2002

On May 22, 1998, President Clinton issued Presidential Decision Directive/PDD-63 (“PDD-63”), which took a broad view of critical infrastructure protection.²³ The directive defined critical infrastructures as “those physical and cyber-based systems essential to the minimum operations of the economy and the government.”²⁴ This definition encompassed a variety of sectors, including, but not limited to, “telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.”²⁵ Historically, many of these infrastructure systems had been separate and independent from each other, both physically and logically;²⁶ however, government documents often refer to critical infrastructure collectively as Critical Infrastructure and Key Resources (“CIKR”).²⁷

²² PDD-63, *supra* note 10, at 1.

²³ See generally *id.*

²⁴ *Id.* at 1.

²⁵ *Id.*

²⁶ *Id.*

²⁷ See, e.g., 2006 NIPP, *supra* note 20; see also U.S. DEP’T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (2007) [hereinafter

Technological advances and increased efficiencies have created a level of interdependence and connectivity between the nation's various critical infrastructures. However, they have created new vulnerabilities as well. PDD-63 expressed President Clinton's intent to eliminate significant weaknesses to both physical and electronic attacks on critical infrastructures, "including especially our cyber systems."²⁸ The directive called for a "closely coordinated effort of both the government and the private sector . . . [that] must be genuine, mutual and cooperative"²⁹ in order to be successful. This initiative marked the advent of public-private partnerships to secure individual sectors of the nation's critical infrastructure by appointing senior officials from designated "Lead Agencies" to work with the private industry in each sector.³⁰

PDD-63 designated the Department of Defense ("DoD") as the Lead Agency for national defense.³¹ Later, the Homeland Security Act of 2002 established the Department of Homeland Security ("DHS") as an executive department of the United States.³² Within DHS, a Directorate for Information Analysis and Infrastructure Protection was created³³ to receive, access, and analyze information received from government agencies as well as the private sector at the national, local, and state levels. The Directorate was to "(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland."³⁴ The Under Secretary for Information Analysis and Infrastructure Protection, leading the Directorate, was also tasked

DIB SSP], available at [*http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf*](http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf).

²⁸ PDD-63, *supra* note 10.

²⁹ *Id.*

³⁰ *Id.* ("For each infrastructure sector that could be a target for significant cyber or physical attack, there will be a single U.S. Government department which will serve as the lead agency for liaison.").

³¹ *See id.*

³² 6 U.S.C. § 111(a) (2006).

³³ *Id.* § 121(a).

³⁴ *Id.* § 121(d)(1).

with several functions involving the synthesis and protection of the information received, including:

- To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States . . .
.
- To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States
- To recommend measures necessary to protect the key resources and critical infrastructure of the United States
- To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States
- To ensure that . . . any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties³⁵

Thus, the Homeland Security Act of 2002 emphasized the protection of the information collected pursuant to DHS's information analysis and infrastructure protection efforts. In addition, the creation of DHS as an executive department resulted in significant implications for cybersecurity, discussed below.

Collaboration between the public and private sectors was again highlighted with the creation of the Protected Critical Infrastructure Information Program ("PCII").³⁶ This information-protection program was established to enhance information sharing between the government and the private sector. Today it is still used to "[a]nalyze and secure critical infrastructure and protected

³⁵ *Id.* § 121(d).

³⁶ See *Protected Critical Infrastructure (PCII) Program*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/editorial_0404.shtm (last visited Oct. 14, 2010).

systems, [i]dentify vulnerabilities and develop risk assessments, and [e]nhance recovery preparedness measures.”³⁷

When information is submitted, from the private sector to the government sector under PCII, it is subjected to the requirements of the Critical Infrastructure Information Act of 2002 (“CII”).³⁸ The specific protections of voluntarily shared critical infrastructure information under the CII are delineated in 6 U.S.C. § 133.³⁹ Under PCII, if the requirements of the Act are met, the information submitted to the government is protected from the Freedom of Information Act,⁴⁰ state and local disclosure laws, and use in civil litigation. The information is also destroyed or returned to the submitter if the enumerated conditions are not met.⁴¹ Thus, even the earliest government cybersecurity initiatives included significant measures to protect information privacy.

2. 2003–2008

In February 2003, the Bush White House issued the National Strategy to Secure Cyberspace, which identified cyberspace as the “nervous system” of the country⁴² and highlighted the role of public-private engagement in securing it.⁴³ The Strategy identifies five national priorities with regard to security in cyberspace: “(1) a national cyberspace security response system; (2) a national cyberspace security threat and vulnerability reduction program; (3) a national cyberspace security awareness and training program; (4) securing governments’ cyberspace; and (5) and national security and international cyberspace security cooperation.”⁴⁴ The second, third, and fourth priorities are targeted toward reducing threats from, and vulnerabilities to cyber attacks.⁴⁵ Under the umbrella of the first listed priority, a national cyberspace security response system, the collaboration between public and private entities is

³⁷ *Id.*

³⁸ Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131–34.

³⁹ *Id.* § 133.

⁴⁰ Freedom of Information Act, 5 U.S.C. § 552.

⁴¹ See *Protected Critical Infrastructure (PCII) Program*, *supra* note 36.

⁴² See NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 20, at iv, 1.

⁴³ *Id.* at 2.

⁴⁴ See *id.* at 3–4.

⁴⁵ *Id.*

again paramount. Among the eight major initiatives in this listed priority, four specifically reference the public-private partnership.⁴⁶

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (“HSPD-7”).⁴⁷ The purpose of HSPD-7 was to establish “a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.”⁴⁸ This directive superseded President Clinton’s Presidential Directive, PDD-63.⁴⁹ HSPD-7 encompassed many initiatives from prior policies, including adequate protection of “voluntarily provided information, . . . that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.”⁵⁰ In addition, DHS and the Sector-Specific Agencies⁵¹ were directed to collaborate with appropriate private sector entities and to encourage information sharing, as well as to “support sector-coordinating mechanisms: (1) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (2) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.”⁵² This directive again attempted to strike a balance between the need for security in cyberspace and the privacy interests of the individual.

⁴⁶ See *id.* The four initiatives are as follows: establishing a public-private architecture for responding to national-level cyber incidents, developing a private sector capability to share a comprehensive view of the potency of cyberspace, coordinating processes for voluntary participation in the development of national continuity and contingency plans, and improving and enhancing public-private information sharing involving cyber threats, vulnerabilities, and attacks. *See id.*

⁴⁷ HSPD-7, *supra* note 20.

⁴⁸ *Id.* ¶ 1.

⁴⁹ *Id.* ¶ 37; *see also infra* Part I.A.1.

⁵⁰ *Id.* ¶ 10.

⁵¹ *Id.* ¶ 6(g) (“The term Sector-Specific Agency means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.”).

⁵² *Id.* ¶ 25.

Most significantly, HSPD-7 directed the DHS Secretary to “produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives.”⁵³ Four specific elements were designated for inclusion in the Plan:

- a. a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;
- b. a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;
- c. a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sectors; and
- d. coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.⁵⁴

These component parts, as well as “other Homeland Security-related elements as the Secretary deems appropriate,”⁵⁵ underlie the formulation of the National Infrastructure Protection Plan (“NIPP”),⁵⁶ released in 2006 and last updated in 2009.⁵⁷

⁵³ *Id.* ¶ 27.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ See 2006 NIPP, *supra* note 20.

⁵⁷ Prior to the release of the completed NIPP in June 2006, many of the initiatives described in the Plan were delineated in additional government documents. *See, e.g.*, U.S. DEP’T OF HOMELAND SEC., THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS (2003), available at http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf; *see also* U.S. DEP’T OF HOMELAND SEC.,

The overarching goal of the NIPP as written in 2006 is, simply stated, to protect the nation's critical infrastructure.⁵⁸ It "provides the unifying structure for the integration of existing and future CIKR protection efforts . . . across sectors" to achieve these security goals on a national level.⁵⁹ Specifically, the NIPP has the objective of "deter[ring] the threat or minimiz[ing] consequences" associated with attacks on the nation's Critical Infrastructure and Key Resources.⁶⁰ It also outlines the roles for security partners in the private and public sectors, including regional partners, the academic community, and government at the state and local level.⁶¹ In accordance with HSPD-7, the NIPP delineates "Sector-Specific Agencies" (replacing the term "Lead Agencies" from prior policy initiatives, but with substantially the same function) to lead efforts in each CIKR sector. DHS, specifically the Office of Cyber Security and Telecommunications, was designated as the Lead Agency for the Information Technology and Telecommunications (now known as the Communications) CIKR sector.⁶²

A risk management framework is the cornerstone of the NIPP approach to CIKR protection, and the plan also recommends implementation using "organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP's goal."⁶³ The "balance between an appropriate level of security and protection of civil rights and liberties" is again highlighted as a goal.⁶⁴ Finally, three larger-scale elements are discussed in the NIPP: the role of CIKR protection in the overall homeland security mission, strategies for ensuring the

INTERIM NATIONAL INFRASTRUCTURE PROTECTION PLAN (2005), available at http://cip.gmu.edu/archive/Interim_NIPP_Feb_05.pdf.

⁵⁸ 2006 NIPP, *supra* note 20, at 1.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ See *id.* at 2.

⁶² See *id.* at 2–3 (Sector-Specific Agencies "implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CI[KR] sectors designated in HSPD-7."); see also *Office of Cybersecurity and Communications*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1185202475883.shtml (last visited May 2, 2010).

⁶³ 2006 NIPP, *supra* note 20, at 4.

⁶⁴ *Id.* at 5.

program's effectiveness and efficiency in the long term, and the provision of resources for the CIKR protection program.⁶⁵

In addition, organizations outside of the government sphere aimed to protect cybersecurity. In December 2008, the Center for Strategic and International Studies ("CSIS") released a report entitled "Securing Cyberspace for the 44th Presidency." CSIS is a bipartisan nonprofit organization that conducts research and analysis, develops policy initiatives, and provides "strategic insights and policy solutions to decision makers."⁶⁶ The report outlined three major findings: cybersecurity is a serious national security problem for the United States; decisions and actions taken with regard to cybersecurity must respect both civil liberties and privacy; and the country will be more secure with a comprehensive national security strategy in place that encompasses both the national and international facets of cybersecurity.⁶⁷

Among the recommendations discussed in the report are several that fall directly in line with the previous directives and policy proposals. First, the CSIS recommended the creation of a national security strategy for cyberspace. It used the acronym DIME—Diplomatic, Intelligence, Military, and Economic—to represent the elements needed for a comprehensive solution.⁶⁸ CSIS also proposed that the White House be placed at the forefront of cybersecurity leadership and create "a new office for cyberspace in the Executive Office of the President."⁶⁹ The role of public-private partnerships was also highlighted; specifically, CSIS suggested that the government "recast" its relationship with the private sector and "redesign" the public-private partnership to include "more clearly defined responsibilities, an emphasis on building trust among the partners, and a focus on operational activities" to increase progress.⁷⁰ CSIS illustrates that non-

⁶⁵ See *id.* at 5–6.

⁶⁶ *About Us*, CTR. FOR STRATEGIC & INT'L STUDIES, <http://csis.org/about-us> (last visited Apr. 10, 2010).

⁶⁷ CENTER FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1 (Dec. 2008), http://csis.org/files/media/csis/pubs/081208_securing_cyberspace_44.pdf.

⁶⁸ *Id.*

⁶⁹ *Id.* at 2.

⁷⁰ *Id.*

governmental organizations have come to some of the same conclusions reached by the government regarding cyberspace security strategy, and it shares the viewpoint that “greater security must reinforce citizens’ rights, not come at their expense.”⁷¹

3. 2009–present

In late 2008, DHS published a notice in the Federal Register describing proposed updates to the National Infrastructure Protection Plan and soliciting public comment “on issues or language in this draft document.”⁷² While the basic framework of the document remained intact, several important changes were introduced, including publication of the sector-specific plans (“SSPs”), updates in information sharing mechanisms, and improvements in other programs led by DHS.⁷³ Somewhat surprisingly, the 2009 NIPP did not contain an abundance of additional information or make significant changes regarding the protection of cyberspace.⁷⁴

On April 17, 2009, the White House Office of the Press Secretary released a statement announcing the conclusion of the sixty-day Cyberspace Review that began on February 9, 2009.⁷⁵ The purpose of the review was “to develop a strategic framework to ensure that our initiatives in [cyberspace] are integrated, resourced and coordinated appropriately, both within the Executive Branch and with Congress and the private sector.”⁷⁶ The conclusion of the review period provided the President with

⁷¹ *Id.* at 15.

⁷² See Review and Revision of the National Infrastructure Protection Plan, 73 Fed. Reg. 67,532 (Nov. 14, 2008), available at <http://edocket.access.gpo.gov/2008/E8-27106.htm>.

⁷³ *Id.*

⁷⁴ Compare 2006 NIPP, *supra* note 20, with U.S. DEP’T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN (2009), available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

⁷⁵ Press Release, White House, Statement by the Press Secretary on Conclusion of the Cyberspace Review (Apr. 17, 2009), available at http://www.whitehouse.gov/the_press_office/Statement-by-the-Press-Secretary-on-Conclusion-of-the-Cyberspace-Review. The Cyberspace Review analyzed “the plans, programs, and activities underway throughout the government that address [the U.S.’s] communication and information infrastructure (i.e. cyberspace).” *Id.*

⁷⁶ *Id.*

conclusions and recommendations for “an optimal White House organizational structure to address cyberspace-related issues and . . . an action plan on identifying and prioritizing further work in this area.”⁷⁷

Just over a month later, on May 29, President Obama addressed the nation on the topic of the security of the United States’ cyber infrastructure.⁷⁸ President Obama reiterated that no single agency has the authority and responsibility to undertake the challenge of securing the country’s cyber networks, and “[n]o single official oversees cybersecurity policy across the federal government.”⁷⁹ The President acknowledged the shortcomings of communication with the private sector and between federal agencies, and announced that his administration would consider digital infrastructure as a “strategic national asset” whose protection is a national security priority.⁸⁰

President Obama also announced the creation of a new Cybersecurity Office within the White House led by the Cybersecurity Coordinator and tasked with the following responsibilities: “orchestrating and integrating all cybersecurity policies for the government; working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities; and, in the event of major cyber incident or attack, coordinating our response.”⁸¹ Public-private partnerships were highlighted once again, as a majority of critical infrastructure is owned by the private sector. However, President Obama emphasized that rather than dictate security standards for private companies, government and industry should work together to find secure technology solutions that promote economic prosperity.⁸² Finally, the President reiterated one of the primary concerns

⁷⁷ *Id.*

⁷⁸ See Remarks by the President, *supra* note 20.

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Id.*; see also *Cybersecurity*, WHITE HOUSE, <http://www.whitehouse.gov/cybersecurity> (last visited Oct. 24, 2010) (“To implement the results of [the *Cyberspace Policy Review*], the President has appointed Howard Schmidt to serve at the U.S. Cybersecurity Coordinator and created the Cybersecurity Office within the National Security Staff . . . ”).

⁸² Remarks by the President, *supra* note 20.

associated with cybersecurity: that civil liberties and privacy remain paramount, and accordingly, that the national cybersecurity plan not subject private sector networks to government monitoring.⁸³

The report following the Cyberspace Policy Review was released in 2009 as a “clean-slate” review of structures and policies for cybersecurity.⁸⁴ It is built upon the same central policy goals as prior initiatives: balancing security and privacy concerns with the promotion of innovation and economic prosperity; strengthening cybersecurity accountability and leadership; and encouraging collaboration between the public and private sectors on an international level.⁸⁵ A significant departure from prior initiatives, however, is the Review’s recommendation that the White House take the lead on cybersecurity-related issues, to demonstrate to the nation and the global community that the United States’ approach to cyberspace protection is a serious response to threats.⁸⁶ This divergence will be analyzed in Part II.A.3 of this Note.

Congress, too, has begun to recognize the importance of cybersecurity as a national concern and has taken action on the legislative side. Senator Jay Rockefeller, for example, proposed the Cybersecurity Act of 2009,⁸⁷ which addresses the finding that the failure to protect cyberspace is one of the most urgent national security problems currently facing the United States and proposes a number of improvements to correct this deficiency, again including public-private collaboration.⁸⁸ The bill has provoked controversy since its introduction was publicized, and at the time of this writing, several other bills have been proposed and are pending in Congress.⁸⁹

⁸³ *Id.*

⁸⁴ CYBERSPACE POLICY REVIEW, *supra* note 20, at iii.

⁸⁵ See *id.*, at iii–v.

⁸⁶ *Id.* at v.

⁸⁷ Cybersecurity Act of 2009, S. 773, 111th Cong. (2009).

⁸⁸ See *id.*

⁸⁹ See Philip Shenon, *Can Obama Shut Down the Internet?*, THE DAILY BEAST (June 18, 2010), <http://www.thedailybeast.com/blogs-and-stories/2010-06-18/new-bill-would-let-obama-police-internet-for-national-security-reasons>; Richard Stiennon, *Rockefeller’s Cybersecurity Act of 2010: A Very Bad Bill*, THE FIREWALL BLOG, FORBES (May 4, 2010,

The most significant proposition from this history of the nation's cybersecurity policies is that while these initiatives have certainly evolved from the Clinton administration to the beginning of the Obama administration, several significant components have remained constant: the continued emphasis on collaboration between the public sector and private industry, the importance of information sharing, and the awareness of the privacy rights and civil liberties of the individual. Part II of this Note will discuss the role of these three elements in the context of the Google-NSA alliance, but in order to better understand this fledgling partnership, its component parts must be considered individually.

B. The Google-NSA Alliance

1. Background Information: Google and the NSA

a) Google

Google's name derives from the word "googol," which is the mathematical term for a 1 followed by 100 zeros as a reflection of the sheer volume of information that exists in the world.⁹⁰ Despite the wide range of products currently offered under the Google name,⁹¹ Google began as a search engine. Today, search still receives the greatest amount of engineering time among the Google products, because Google believes that the search engine can always be improved.⁹² This falls squarely in line with Google's mission: "to organize the world's information and make it universally accessible and useful."⁹³

i. Google's Privacy Policies and Data Collection Methods

The expansion of Google's services has led to increasing concerns about the privacy of Google's individual users. Google's

12:43 PM), <http://blogs.forbes.com/firewall/2010/05/04/rockefellers-cybersecurity-act-of-2010-a-very-bad-bill>.

⁹⁰ *Corporate Information, Company Overview*, GOOGLE, <http://www.google.com/corporate/index.html> (last visited Apr. 10, 2010) [hereinafter *Company Overview*].

⁹¹ See *More Google Products*, GOOGLE, <http://www.google.com/intl/en/options/> (last visited Apr. 10, 2010) (listing Gmail, Maps, Docs, Calendar, and Reader, among Google services).

⁹² *Company Overview*, *supra* note 90.

⁹³ *Id.*

privacy policy applies to products, services, and websites offered by Google, Inc. or its affiliated companies and subsidiaries.⁹⁴ Collectively, these are known as Google’s “services,” and Google “post[s] supplementary privacy notices as needed to describe how specific services process personal information.”⁹⁵ An individual user is asked to provide specific personal information to Google, such as a name, an e-mail address, and an account password for those services that require registration.⁹⁶

Google’s servers automatically record “log information,” also known as “server logs,” when a user accesses Google services.⁹⁷ This information could include a user’s web request, browser type, Internet Protocol (“IP”) address, date and time of request, browser language, and one or more “cookies” that may uniquely identify that user’s browser.⁹⁸ The privacy policy also states that Google may also retain e-mail or other communications sent to the company in order to process user inquiries, respond to user requests, and improve its services.⁹⁹ Google’s privacy policy applies to personal information provided to affiliated Google services on other sites. Thus, information provided to affiliated services is protected under Google’s privacy policy. However, the policy also cautions that affiliated web sites may have different privacy practices and encourages users to review those sites’ policies.¹⁰⁰

⁹⁴ *Privacy Policy*, GOOGLE (Mar. 11, 2009), http://www.google.com/intl/en/privacy_archive.html [hereinafter *Google Privacy Policy*] (follow “Version 03/11/2009”).

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.* A “cookie” is a small file containing a string of characters that is sent to a computer or other device uniquely identifying the user’s Internet browser when the user visits Google. Cookies are used to improve the quality of Google’s service, including improvements in search results and ad selection, storing user preferences, and tracking user trends, such as how users search. Cookies are also used in advertising services to help publishers and advertisers manage ads across the Internet, so when a user visits a website and views or clicks on an ad supported by Google’s advertising services, including Google sites using advertising cookies, one or more cookies may be set in that user’s Internet browser. *What are Computer Cookies?*, WISEGEEK, <http://www.wisegeek.com/what-are-computer-cookies.htm> (last visited Sept. 14, 2010).

⁹⁹ *Google Privacy Policy*, *supra* note 94.

¹⁰⁰ *Id.*

Google also emphasizes that personal information is processed for the limited purposes described within their privacy policy “and/or the supplementary privacy notices for specific services,”¹⁰¹ as well as other additional purposes, including: “providing our services, including the display of customized content and advertising; auditing, research, and analysis in order to maintain, protect, and improve our services; ensuring the technical functioning of our network; protecting the rights or property of Google or our users and developing new services.”¹⁰²

The most significant take away from Google’s privacy policy is that it applies to Google services only. Google does not “exercise control over the sites displayed in search results, sites that include Google applications, products or services, or links from within our various services.”¹⁰³

ii. Information Sharing, Security, and Data Integrity

Google only shares personal information provided by a user with other companies or individuals under limited circumstances.¹⁰⁴ First, a user must consent for the sharing of any sensitive personal information, and Google only provides the information to Google’s “subsidiaries, affiliated companies, or other trusted businesses or persons for the purposes of processing personal information.”¹⁰⁵ These parties must agree to process this information based on Google’s instructions, in compliance with Google’s privacy policy, and any other appropriate security and confidentiality measures.¹⁰⁶ Google also shares personal information with outside companies where there is a good faith belief that:

access, use, preservation, or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable government request, (b) enforce applicable Terms of Service, including investigation

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security, or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.¹⁰⁷

Should Google be involved in a merger, acquisition, or sale of all or part of its assets, Google will “provide notice before personal information is transferred and becomes subject to a different privacy policy.”¹⁰⁸ Google will also make certain that personal information involved in such transactions remains confidential.¹⁰⁹ Certain aggregated, non-personal information (such as the numbers of users who searched a certain term or clicked on a particular advertisement) may be shared with third parties without identifying individual users.¹¹⁰ Google takes “security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data . . . [including] internal reviews of data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where [it] store[s] personal data.”¹¹¹ Google heavily restricts unauthorized access to personal information.¹¹²

Personal information provided to Google is processed in accordance with the company’s privacy policies.¹¹³ Google only uses the information for its collected purpose, and Google reviews its storage, collection, and processing practices regularly to ensure that only the minimum amount of personal information needed to provide or improve Google services is collected, stored, and processed.¹¹⁴ Finally, Google will work with both individual users

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² See *id.* Google employees, agents, and contractors are bound by confidentiality obligations and subject to discipline for non-compliance, and these individuals require some access to personal information to develop, improve, and operate Google systems.

Id.

¹¹³ See *id.*

¹¹⁴ *Id.*

and regulatory authorities, if necessary, to respond to formal written complaints regarding concerns involving the transfer of personal data.¹¹⁵

Several changes to Google's privacy policy were implemented beginning October 3, 2010, and users were notified of these changes prior to the application of the new policy.¹¹⁶ While the majority of the policy remains the same as discussed above, Google deleted twelve product-specific policies so that more Google products and services are governed by one privacy policy; and Google modified the overall policy to reduce redundancies and simplify the legal language to make it easier to understand.¹¹⁷ Google also created a web page detailing the specific additions and omissions since the last update of the policy on March 11, 2009.¹¹⁸

Despite its robust privacy protection policy, Google was recently involved in a serious privacy breach. In May 2010, Google announced on its official blog and on its European Public Policy blog that some data collected by Google Street View cars for use in location-based products, such as Google Maps for mobile phones, mistakenly included "payload data" (information sent over a wireless network) from open wireless Internet networks, meaning those that are not protected by a password.¹¹⁹ Payload data includes bits of personal data sent over these unencrypted networks.¹²⁰ The European Public Policy blog post originally stated that no payload data was collected from such networks; rather, only publicly broadcast information like the name of the wireless network and the MAC address, which is the unique number assigned to a device such as a wireless router, was

¹¹⁵ *Id.*

¹¹⁶ Mike Yang, *Trimming Our Privacy Policies*, OFFICIAL GOOGLE BLOG (Sept. 3, 2010, 9:00 AM), <http://googleblog.blogspot.com/2010/09/trimming-our-privacy-policies.html>.

¹¹⁷ *Id.*; see also *Privacy Policies Update-FAQ*, GOOGLE, http://www.google.com/privacy_faq_2010.html (last visited Oct. 2, 2010).

¹¹⁸ *Privacy Policy Update*, GOOGLE, http://www.google.com/privacy_changes_2010.html (last visited Oct. 2, 2010).

¹¹⁹ Alan Eustace, *WiFi Data Collection: An Update*, OFFICIAL GOOGLE BLOG (May 14, 2010, 1:44 PM), <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>; Peter Fleischer, *Data Collected by Google Cars*, GOOGLE EUROPEAN PUBLIC POLICY BLOG (Apr. 27, 2010, 1:01 PM), <http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html>.

¹²⁰ Eustace, *supra* note 119.

obtained.¹²¹ A flurry of criticism followed both the original announcement and the update including the admission of this mistake, and could affect the public's perception of Google's ability to keep personal data secure and private.¹²² In June 2010, it was announced that Connecticut Attorney General and Senator-elect¹²³ Richard Blumenthal would be leading a thirty-state investigation into Google's Wi-Fi gathering scandal.¹²⁴ Several countries other than the United States, including Spain, have begun their own inquiries.¹²⁵

Notwithstanding this incident, Google is still ranked the number one most visited website in the world according to three-month Internet traffic rankings conducted by Alexa,¹²⁶ a web information company that maintains a database of statistics and other related information about popular Web sites.¹²⁷

¹²¹ Fleischer, *supra* note 119.

¹²² See, e.g., Cecilia Kang, *Growing Anger Over Google Street View Privacy Breach*, POST TECH. BLOG, WASHINGTONPOST.COM (May 20, 2010, 8:00 PM), http://voices.washingtonpost.com/posttech/2010/05/the_anger_is_growing_over.html; Cecilia Kang, *Lawmakers Press FTC on Google Street View Privacy Lapse*, POST TECH. BLOG, WASHINGTONPOST.COM (May 19, 2010, 3:19 PM), http://voices.washingtonpost.com/posttech/2010/05/us_lawmakers_press_ftc_on_inve.html; Xeni Jardin, *Google: We Inadvertently Collected Personal Data Sent over WiFi Networks*, BOING BOING (May 16, 2010), <http://www.boingboing.net/2010/05/14/google-yes-we-snoope.html>; Jason Kincaid, *Google Admits to Accidentally Collecting Personal Data With Street View Cars*, TECHCRUNCH (May 14, 2010), <http://techcrunch.com/2010/05/14/google-admits-to-accidentally-collecting-personal-data-with-street-view-cars>; Ross Miller, *Street View Cars Mistakenly Nabs Personal Data over WiFi Networks, Says Google*, ENGADGET (May 14, 2010, 7:51 PM), <http://www.engadget.com/2010/05/14/street-view-cars-mistakenly-nabs-personal-data-over-wifi-says-g>; Kim Zetter, *Google Street View Cams Collected Private Content from WiFi Networks*, THREAT LEVEL BLOG, WIRED (May 15, 2010, 7:15 PM), <http://www.wired.com/threatlevel/2010/05/google-street-view-cams>.

¹²³ David M. Halbfinger, *Blumenthal Wins in Connecticut to Take Dodd's Senate Seat*, N.Y. TIMES, Nov. 2, 2010, at P12, available at <http://www.nytimes.com/2010/11/03/nyregion/03ctsen.html>.

¹²⁴ See, e.g., Scott Morrison, *Connecticut to Lead Multi-State Probe of Google*, WALL ST. J., June 21, 2010, <http://online.wsj.com/article/SB10001424052748704895204575320802269077146.html>; Tom Krazit, *Connecticut Heads up 30-State Google Wi-Fi Probe*, CNET (June 21, 2010, 11:46 AM), http://news.cnet.com/8301-30684_3-20008332-265.html.

¹²⁵ E.g., Raphael Minder, *Google Sued in Spain over Data Collection*, N.Y. TIMES, Aug. 17, 2010, <http://www.nytimes.com/2010/08/18/technology/18google.html>.

¹²⁶ *Google.com Site Info*, ALEXA, <http://www.alexa.com/siteinfo/google.com> (last visited Nov. 21, 2010).

¹²⁷ *Alexa Internet, Company Overview*, ALEXA, <http://www.alexa.com/company> (last visited Nov. 21, 2010).

Nevertheless, the amount of data involved in this Wi-Fi breach is relatively small compared to the volume of data the company handles on a routine basis.¹²⁸ Google has also been subjected to negative publicity in the past without a significant deterrent effect on its overall usage.¹²⁹

b) The National Security Agency

The National Security Agency was established, by order of President Harry S. Truman on November 4, 1952, in the wake of government work breaking enemy codes during World War II, which was a significant contributing factor in winning the war.¹³⁰ The establishment of the NSA followed several government studies determining how best to continue codebreaking work after World War II.¹³¹ The Central Security Service (“CSS”), established by Presidential Directive in 1972, includes the elements of the armed forces (Navy, Air Force, Army, Coast Guard, and Marine Corps) that engage in codemaking and codebreaking work along with the NSA.¹³² The CSS and the NSA members work together around the world to support both military and civilian leaders, as well as the White House, policy and decision makers, and troops at the front lines.¹³³ The government-wide responsibilities of the NSA/CSS render it unique among the defense agencies because it provides products and services to the Department of Defense, government agencies, industry partners, the Intelligence Community, and select allies and coalition partners; it also delivers critical strategic and tactical information to war planners and fighters.¹³⁴ Specifically, “NSA/CSS provides

¹²⁸ See *Google Transparency Report: Traffic*, GOOGLE, <http://www.google.com/transparencyreport/traffic> (last visited Nov. 21, 2010). “This tool provides information about [Internet] traffic to [Google] services around the world. Each graph shows historic traffic patterns for a given country/region and service.” *Id.*

¹²⁹ See, e.g., *Google Ranked “Worst” on Privacy*, BBC NEWS, June 11, 2007, <http://news.bbc.co.uk/2/hi/technology/6740075.stm>.

¹³⁰ *Frequently Asked Questions About NSA*, NAT’L SEC. AGENCY § 1 (Jan. 15, 2009), http://www.nsa.gov/about/faqs/about_nsa.shtml [hereinafter *FAQ About NSA*] (follow “How and When Was the National Security Agency Established?”).

¹³¹ *Id.*

¹³² *Id.* (follow “What Is the Central Security Service?”).

¹³³ *Id.*

¹³⁴ *Id.*

intelligence products and services to the White House, executive agencies (such as CIA and the State Department), the Chairman and Joint Chiefs of Staffs (JCS), military combatant commanders and component commands, military departments, multinational forces, and U.S. allies.”¹³⁵ In addition, it provides Information Assurance products and services to government contractors and users of national security information systems.¹³⁶

The National Security Agency has two core missions: to protect the national security systems of the United States and to produce information about foreign intelligence.¹³⁷ The NSA/CSS has two interconnected missions: Information Assurance (“IA”), through which the national security information systems and information of the United States are protected from theft or damage; and Signals Intelligence (“SIGINT”), which “gather[s] information that America’s adversaries wish to keep secret.”¹³⁸ SIGINT collects foreign intelligence from various sources, interprets it (often deciphering foreign languages, dialects, and security codes), and provides it to customers throughout the United States government, which uses the information to advance national objectives, including fighting terrorism and protecting military troops.¹³⁹ Information Assurance prevents unauthorized access to classified or sensitive national security information, both by keeping information safe from unlawful access and ensuring that the information needed by our decision makers is available and reliable.¹⁴⁰ These two missions assist the function of enabling a military operation known as Network Warfare.¹⁴¹ In carrying out these missions, the NSA/CSS defends vital networks, saves lives, and advances the alliances and goals of the United States.¹⁴² Privacy rights guaranteed by the Constitution and the laws of the

¹³⁵ *Id.* (follow “Who Are the NSA/CSS’ Customers?”).

¹³⁶ *Id.*

¹³⁷ See *id.*; see also *The NSA/CSS Mission*, NAT'L SEC. AGENCY, <http://www.nsa.gov/about/mission/index.shtml> (last visited May 2, 2010).

¹³⁸ *FAQ About NSA*, *supra* note 130 (follow “What Does the NSA/CSS Do?”).

¹³⁹ *Id.* (follow “What is Signals Intelligence?”).

¹⁴⁰ *Id.* (follow “What is Information Assurance?”).

¹⁴¹ See *id.* (follow “Who Are the NSA/CSS’ Customers?”).

¹⁴² *Id.*

United States remain strictly protected in the execution of these missions.¹⁴³

2. Events Prompting the Formation of the Google-NSA Alliance

On January 12, 2010, Google posted an announcement entitled *A New Approach to China* on its official blog.¹⁴⁴ The posting publicized the fact that in mid-December 2009, a “highly sophisticated and targeted attack on [Google’s] infrastructure originating from China . . . resulted in the theft of intellectual property from Google.”¹⁴⁵ Google highlighted that the attack did not specifically target Google; the blog post explicitly stated that “at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media, and chemical sectors” were also targeted. Nevertheless, a primary goal of the Google attack was to gain access to the Gmail¹⁴⁶ accounts of Chinese human rights activists.¹⁴⁷ Investigations thus far led Google to believe that this objective was not achieved because only two accounts appeared to have been accessed, and the “activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.”¹⁴⁸

Independent of this particular attack, but still relevant to Google’s investigation, was the discovery that dozens of Gmail accounts (from users in the United States, Europe, and China) belonging to advocates for human rights in China appeared to have been accessed by third parties on a routine basis.¹⁴⁹ Google

¹⁴³ *Id.*

¹⁴⁴ See David Drummond, *A New Approach to China*, OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html> [hereinafter Drummond, *A New Approach to China*].

¹⁴⁵ *Id.*

¹⁴⁶ Gmail is Google’s webmail service. See *What Is Gmail?*, GMAIL HELP, <http://mail.google.com/support/bin/answer.py?hl=en&answer=6554> (last visited Oct. 14, 2010).

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Id.*

speculated that the accounts were accessed via “phishing” scams¹⁵⁰ or “malware”,¹⁵¹ placed on a user’s computer, not through a security breach at Google.¹⁵² The information gained from this attack prompted Google to improve its systems for enhanced security on the part of Google and its user.¹⁵³

Google recommended that users take precautions to protect themselves in cyberspace (such as deploying anti-virus and anti-spyware programs¹⁵⁴ on their computers, installing patches for their computer operating systems,¹⁵⁵ and updating their Internet browsers).¹⁵⁶ The blog post cautioned against clicking on hyperlinks that appear in instant messages or e-mails, and sharing personal information like passwords; it also provided a link to further information on specific cybersecurity recommendations.¹⁵⁷

¹⁵⁰ See *What Is a Phishing Scam?*, WISEGEEK, <http://www.wisegeek.com/what-is-a-phishing-scam.htm> (last visited Oct. 14, 2010) (“A phishing scam is an identity theft scam that arrives via email. The email appears to originate from a legitimate source such as a trusted business or financial institution and includes an urgent request for personal information,” typically invoking a critical need to update an account immediately. When a user clicks on a link in the email, s/he is directed to an official-looking website, but any personal information provided to this site is sent directly to the scam artist.).

¹⁵¹ Malware is an abbreviation used to refer to a malicious software program. See *What is Malware?*, WISEGEEK, <http://www.wisegeek.com/what-is-malware.htm> (last visited Oct. 14, 2010).

¹⁵² Drummond, *A New Approach to China*, *supra* note 144.

¹⁵³ *Id.*

¹⁵⁴ Anti-virus software programs detect and remove computer viruses, and anti-spyware programs remove spyware software from computers. Spyware covertly gathers information about a user’s Internet use and transmits that information to a third party individual or company that uses it for marketing or other purposes. See *Antivirus Software*, DICTIONARY.COM, <http://dictionary.reference.com/browse/antivirus+software> (last visited May 2, 2010); *Spyware*, DICTIONARY.COM, <http://dictionary.reference.com/browse/spyware> (last visited May 2, 2010); see also *Do I Need a Spyware Blocker in Addition to Antivirus Software?*, WISEGEEK, <http://www.wisegeek.com/do-i-need-a-spyware-blocker-in-addition-to-antivirus-software.htm> (last visited May 2, 2010).

¹⁵⁵ A computer’s operating system (abbreviated as “OS”) is a program “designed to run other programs on a computer.” *What Is an Operating System?*, WISEGEEK, <http://www.wisegeek.com/what-is-an-operating-system.htm> (last visited May 2, 2010). Software companies often issue “patches” between releases of operating systems, to temporarily correct a flaw in the software until a new version of the OS is released. See *What Is a Software Patch?*, WISEGEEK, <http://www.wisegeek.com/what-is-a-software-patch.htm> (last visited May 2, 2010).

¹⁵⁶ Drummond, *A New Approach to China*, *supra* note 144.

¹⁵⁷ *See id.*

Additional links were supplied for those interested in learning more about these kinds of attacks.¹⁵⁸

Google explained that it had shared the information about the attacks with the world due to the security and human rights implications of the information uncovered, but also because of its significance with regard to the global debate about freedom of speech.¹⁵⁹ In light of China's economic development over the past twenty years, Google.cn was launched in January 2006 with the belief that any discomfort on Google's part in agreeing to censor some search results was substantially outweighed by "the benefits of increased access to information for people in China and a more open Internet."¹⁶⁰ The recent attacks and the surveillance they uncovered, as well as China's continued attempts to further limit free speech on the Internet, led Google to review the feasibility of its business operations in China. Google concluded that it was no longer willing to continue censoring its results on Google.cn, and announced that it would be discussing the possibility of operating an unfiltered search engine on Google.cn with the Chinese government.¹⁶¹

On February 4, 2010, the *Washington Post* reported that Google and the National Security Agency had partnered to analyze

¹⁵⁸ These links included a report to Congress by the U.S.-China Economic and Security Review Commission ("USCC"), a related analysis prepared for the USCC, a presentation on the GhostNet spying incident, and a blog written by Nart Villaneuve, a self-described "Internet Censorship Explorer." See U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2009 REPORT TO CONGRESS (November 2009), available at http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf; BRIAN KREKEL, NORTHROP GRUMMAN, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION REPORT ON THE CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION (Oct. 9, 2009), available at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf; TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK, INFORMATION WARFARE MONITOR (Mar. 29, 2009), available at <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network> (describing GhostNet as a suspected cyber espionage network of over 1,295 infected computers in 103 countries, 30% of which are high-value targets, including ministries of foreign affairs, embassies, international organizations, news media, and NGOs); NART VILLANEUVE, <http://www.nartv.org> (last visited Apr. 13, 2010).

¹⁵⁹ Drummond, *A New Approach to China*, *supra* note 144.

¹⁶⁰ *Id.*

¹⁶¹ *Id.*

2010]

CYBERSECURITY AT INTERNET SPEED

201

the cyberattacks, with the objective of better defending Google and its users from future attack.¹⁶² Though neither organization commented on the partnership, sources told the *Washington Post* that the alliance allows for the sharing of critical information without violating Google's policies or laws that protect Americans' privacy of online communications. Under the terms of the alliance, Google will not be sharing proprietary data and the NSA will not be viewing users' searches or e-mail accounts.¹⁶³ The article stated that Google approached the NSA shortly after the attacks, but due to the sensitivity of the alliance, the deal took time to be formulated.¹⁶⁴ Any agreement would be the first instance where Google had entered a "formal information-sharing relationship" with the NSA; in 2008 the company stated that it had not cooperated with the NSA's Terrorist Surveillance Program.¹⁶⁵ Sources also said that the focus of the alliance is to better defend Google's networks and prevent future attacks, as it would be nearly impossible to determine the specific origins of the recent attack after the fact.¹⁶⁶

An NSA spokesperson said that the organization works with many "commercial partners and research associates to ensure the availability of secure tailored solutions for Department of Defense and national security systems customers," but Google's broad reach and global presence make it unique among the NSA's clients.¹⁶⁷ This alliance allows the NSA to help Google evaluate vulnerabilities in its hardware and software to assist in its defenses, determine the level of sophistication of the adversary, utilize the analysis performed by the NSA in prior attacks to help prevent future incidents, and learn what methods were used to infiltrate Google's system.¹⁶⁸ Google, in turn, may share details about the malicious code used to attack Google's system, without revealing

¹⁶² Ellen Nakashima, *Google to Enlist NSA to Ward Off Attacks; Firm Won't Share User Data, Sources Say, But Deal Raises Issue of Privacy vs. Security*, WASH. POST, Feb. 4, 2010, at A1.

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*

proprietary data about the intellectual property that was taken, as this disclosure likely would perturb shareholders and subject the company to public scrutiny and possibly legal action.¹⁶⁹

The New York Times reported a similar story about the Google-NSA alliance the following day, containing many of the same facts as the *Washington Post* article, as well as several significant additions.¹⁷⁰ *The New York Times* piece reported that Google was partnering with the NSA rather than DHS because the former has “no statutory authority to investigate domestic criminal acts,” while the latter has such authority.¹⁷¹ By partnering with the NSA, then, Google can prevent the government from regulating its search engine, e-mail, and other services as part of the nation’s “critical infrastructure.”¹⁷² *The New York Times* called the alliance a “cooperative research and development agreement,” which is a specific category created under the Federal Technology Transfer Act of 1986¹⁷³ that describes a written agreement between a government agency and a private company to collaborate on a particular project with the goal of accelerating the commercialization of government-developed technology.¹⁷⁴ The article also revealed that Google was working with the Federal Bureau of Investigation to inquire into the attack, but the bureau made no public comment about the incident.¹⁷⁵ Similarly, the NSA has never issued a formal comment on the existence of an alliance with Google or any of the details mentioned in the initial news releases. By contrast, the agency has issued official comments on at least one other occasion to correct inaccurate portrayals of its initiatives in the media.¹⁷⁶

¹⁶⁹ *Id.*

¹⁷⁰ See John Markoff, *Google Asks Spy Agency for Help with Inquiry Into Cyberattacks*, N.Y. TIMES, Feb. 5, 2010, at A6, available at <http://www.nytimes.com/2010/02/05/science/05google.html>.

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ Federal Technology Transfer Act of 1986, 15 U.S.C. § 3710 (2006).

¹⁷⁴ Markoff, *supra* note 170.

¹⁷⁵ *Id.*; see *infra* Part II of this Note for a discussion of the commentary and criticisms that followed Google’s announcement.

¹⁷⁶ See Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL STREET J., July 8, 2010, http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704545004575352983850463108.html; see also Tony Bradley, *NSA “Perfect*

In mid-February, *The New York Times* reported that the Google cyber attacks had been “traced to computers at two educational institutions in China,” one of which has close ties to the Chinese military.¹⁷⁷ The article stated that the attacks may have begun months earlier than previously believed and that the goals of the attacks were to steal trade secrets and computer codes, and to access the e-mail accounts of Chinese human rights activists.¹⁷⁸ The two schools involved were Shanghai Jiaotong University, home of one of China’s top computer science programs, and the Lanxiang Vocational School, which was established with military support and is responsible for training some of China’s military computer scientists.¹⁷⁹

Spokespeople from the schools said that they had not heard that the attacks on Google had been traced to their campuses. However, computer security analysts theorize that the vocational schools were used as a cover for government operations, that a third country may have been involved, and that the hacking was criminal industrial espionage with the goal of stealing intellectual property from American technology firms.¹⁸⁰ Independent researchers monitoring Chinese information warfare caution that China has adopted a “highly distributed approach to online espionage” which renders proof of the origin of an attack nearly impossible to discover.¹⁸¹

On March 22, 2010, Google posted an update on its official blog announcing that it would no longer censor its search services

Citizen Program Is Only One Piece of Cyber Security Puzzle, PC WORLD (July 9, 2010, 7:55 AM), http://www.pcworld.com/businesscenter/article/200768/nsa_perfect_citizen_program_is_only_one_piece_of_cyber_security_puzzle.html (discussing the official response to the “Perfect Citizen” program as characterized by the Wall Street Journal, issued by a NSA spokesperson via e-mail).

¹⁷⁷ John Markoff & David Barboza, 2 China Schools Said to Be Tied to Online Attacks, N.Y. TIMES, Feb. 19, 2010, at A1, available at <http://www.nytimes.com/2010/02/19/technology/19china.html>.

¹⁷⁸ *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ *Id.* The theory suggesting involvement on the part of the Chinese government is corroborated by the documents made public by WikiLeaks on November 28, 2010. See Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 28, 2010, <http://www.nytimes.com/2010/11/29/world/29cables.html>.

¹⁸¹ *Id.*

on Google.cn.¹⁸² “[T]hese attacks and the surveillance they uncovered—combined with attempts over the last year to further limit free speech on the web in China including the persistent blocking of websites such as Facebook, Twitter, YouTube, Google Docs and Blogger”—led Google to cease censorship of search results on Google.cn.¹⁸³ From March 22 onward, visitors to Google.cn were automatically redirected to Google.com.hk and received the same uncensored search results (including Google Search, Google News, and Google Images) as users of the Hong Kong Google site. The site was presented in simplified Chinese designed for users in China, but the search results were delivered via Google servers in Hong Kong.¹⁸⁴

Google argued that the switch to Google.com.hk was a legal and appropriate way to allow further access to Google services in mainland China.¹⁸⁵ However, the Chinese government continued to insist that Internet censorship was a non-negotiable legal requirement of operating in their country. Google was thus aware that the Chinese government could block access to Google’s web services at any time.¹⁸⁶ Accordingly, a new web page was created to detail which Google services are available in China for any given date and time.¹⁸⁷

Several days later, the large Internet domain registration company Go Daddy changed its policy and began discontinuing new “.cn” domain registrations¹⁸⁸ in China.¹⁸⁹ Though Go Daddy said that the decision to discontinue selling .cn names had nothing

¹⁸² David Drummond, *A New Approach to China: An Update*, OFFICIAL GOOGLE BLOG (Mar. 22, 2010, 12:03 PM), <http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html> [hereinafter Drummond, *A New Approach to China: An Update*].

¹⁸³ *Id.*

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*; see also Miguel Helft & David Barboza, *Google Will Redirect China Users to Hong Kong Site*, N.Y. TIMES, Mar. 23, 2010, at A1, available at <http://www.nytimes.com/2010/03/23/technology/23google.html>.

¹⁸⁶ See Helft & Barboza, *supra* note 185.

¹⁸⁷ Drummond, *A New Approach to China: An Update*, *supra* note 182.

¹⁸⁸ See *What is Domain Registration?*, WISEGEEK, <http://www.wisegEEK.com/what-is-domain-registration.htm> (last visited May 2, 2010).

¹⁸⁹ Geoffrey A. Fowler, *What Does it Cost Go Daddy To Leave China?*, WALL ST. J. BLOG, DIGITS (Mar. 24, 2010, 11:15 PM), <http://blogs.wsj.com/digits/2010/03/24/what-does-it-cost-go-daddy-to-leave-china>.

to do with publicity or with Google's movement of searches into Hong Kong,¹⁹⁰ movement by these two major companies out of China clearly demonstrates China's serious and continual threat to United States cybersecurity. This is especially evident because in June 2010, Google's license to operate in China was at risk of not being renewed. On June 28, 2010, Google announced on its official blog that it would no longer automatically direct users to the uncensored Hong Kong site; rather, in an apparent compromise to appease the Chinese government, users of the Google.cn site saw a page that allowed them to proceed to the Hong Kong site if they wished.¹⁹¹ An additional blog update on July 9, 2010 confirmed that web search and other Google products remain available to users in China.¹⁹²

These events following the Google attacks are pertinent to the U.S. government's attempts to balance its own security needs with the privacy rights of the individual Internet user. China represents one extreme of the spectrum, with a high level of government involvement in cyberspace security, such that the rights of the individual have been largely stifled.¹⁹³ As a result, private companies like Google and Go Daddy have decided to discontinue or modify their services there.¹⁹⁴ The other extreme would entail little to no government involvement in the security of cyberspace, which surely would lead to increased cyberattacks. Part II of this Note will discuss the effectiveness of the current cybersecurity strategy articulated by the U.S. government, in the context of

¹⁹⁰ *Id.* Christine Jones, General Counsel of the Go Daddy Group, made these statements during an interview following her testimony at a hearing before the Congressional-Executive Commission in Washington, D.C. *Id.*

¹⁹¹ David Drummond, *An Update on China*, OFFICIAL GOOGLE BLOG (Jun. 28, 2010, 10:45 PM), <http://googleblog.blogspot.com/2010/06/update-on-china.html> [hereinafter Drummond, *An Update on China*]; Keith B. Richburg, *Google Compromise Pays Off with Renewal of License in China*, WASH. POST, July 10, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/09/AR2010070902137.html>; see also *China's Renewal of Google's License Offers Hope of Resisting Censorship*, WASH. POST, July 14, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071305390.html>.

¹⁹² See Drummond, *An Update on China*, *supra* note 191 (last updated July 9, 2010).

¹⁹³ Drummond, *A New Approach to China: An Update*, *supra* note 182.

¹⁹⁴ See *supra* Part I.B.2.

whether the Google-NSA alliance represents continuity and is demonstrative of its effectiveness.

II. IF GOOGLE IS APPROACHING THE NSA TO PROTECT ITSELF, ARE CURRENT GOVERNMENT POLICIES PROVING INEFFECTIVE?

As discussed in Part I.B of this Note, very few details have been made public about the Google-NSA alliance. This Part will discuss the commentary and criticisms that have followed the announcement of the partnership. This Part will also present two competing arguments: that the formation of the alliance reveals the ineffectiveness of the government's cybersecurity regime and highlights the shortcomings of existing policies; and that the alliance represents the type of partnership envisioned by current cybersecurity initiatives and demonstrates the effectiveness of these policies.

A. *The Google-NSA Alliance Is a Marked Departure from Current Policy and Demonstrative of its Ineffectiveness*

Privacy is at the heart of the discussion about the Google-NSA alliance. Despite the benefits of the alliance discussed in Part II.B, privacy organizations such as the American Civil Liberties Union ("ACLU") and the Electronic Privacy Information Center¹⁹⁵ have heavily criticized Internet privacy policies generally, as well as Google's policy specifically, for its insufficient protection of users. These concerns play an important role in view of the Google-NSA alliance as a significant departure from the government's stated cybersecurity policies.

1. The NSA Is the Designated Government Agency

Since 2002, DHS has been at the forefront of national security matters, and was designated as the Lead Agency for the technology sector in the National Infrastructure Protection Plan.¹⁹⁶ By

¹⁹⁵ See *Technology and Liberty*, AM. CIVIL LIBERTIES UNION, <http://www.aclu.org/technology-and-liberty> (last visited Sept. 15, 2010); see also *Cybersecurity Privacy Policy Implications*, ELEC. PRIVACY INFO. CTR., <http://epic.org/privacy/cybersecurity/default.html> (last visited Sept. 15, 2010).

¹⁹⁶ 2006 NIPP, *supra* note 20, at 3.

2010]

CYBERSECURITY AT INTERNET SPEED

207

contrast, the NSA is not mentioned by name in the NIPP as a Sector-Specific Agency for any critical infrastructure sector.¹⁹⁷ Its inclusion as the de facto lead government agency in its partnership with Google is thus a significant departure from stated government policies regarding CIKR protection. Though DHS was designated as the Sector-Specific Agency for both the Information Technology sector and Communications sector, the NIPP indicates that organizations like the NSA that “have unique responsibilities, functions, or expertise in a particular CI[]KR sector”¹⁹⁸ may still play an important, but secondary role in CIKR protection efforts without Sector-Specific Agency designation. Specifically, such organizations “will [a]ssist in assessing risk, prioritizing CI[]KR, and enabling protective actions and programs within that sector; [s]upport the national goal of enhancing CI[]KR protection . . . and [c]ollaborate with all relevant security partners to share security-related information within the sector, as appropriate.”¹⁹⁹

Experts in this field also see a broader role for the NSA in protecting the nation’s critical infrastructure. Larry M. Wortzel, the Vice Chairman of the U.S.-China Economic and Security Review Commission, stated in his testimony before the Senate Judiciary Subcommittee on Terrorism and Homeland Security that the NSA should be at the forefront of cyber efforts, as opposed to DHS or another government agency, for several significant reasons.²⁰⁰ Wortzel cited the NSA’s “strong institutional culture of adherence to the Foreign Intelligence and Surveillance Act”²⁰¹ and emphasized that agency personnel are unique from other members of the intelligence community because in addition to being “skilled and superbly trained,” they “are trained to protect the privacy and

¹⁹⁷ See *id.*

¹⁹⁸ *Id.* at 22.

¹⁹⁹ *Id.*

²⁰⁰ *Preventing Terrorist Attacks and Protecting Privacy in Cyberspace Before the Senate Judiciary Subcomm. on Terrorism and Homeland Security*, 111th Cong. (2009) (statement of Larry Wortzel, Vice Chairman, U.S.-China Economic and Security Review Commission) [hereinafter *Wortzel Testimony*], available at http://judiciary.senate.gov/hearings/testimony.cfm?id=4169&wit_id=8316.

²⁰¹ *Wortzel Testimony*, *supra* note 200; see also Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885 (2006); *Foreign Intelligence Surveillance Act (FISA)*, CTR. FOR NAT’L SEC. STUDIES, <http://www.cnss.org/fisa.htm> (last visited Sept. 15, 2010).

rights of American persons” and the NSA is the only agency with “decades of experience . . . conducting operations in the electronic and cyber realms.”²⁰² The NSA also has “broad international contacts with allies and friendly governments[,] . . . wide contacts in the private sector. . . [and] a cadre of highly skilled linguists able to work in the languages associated with the origin of the foreign intrusions.”²⁰³

Mike McConnell, director of the NSA under the Clinton administration, also supports the NSA’s leadership within the realm of cybersecurity.²⁰⁴ McConnell asserts in an article published in the *Washington Post* that the NSA “is the only agency in the United States with the legal authority, oversight, and budget dedicated to breaking the codes and understanding the capabilities and intentions of potential enemies.”²⁰⁵ Google’s decision to approach the NSA rather than DHS for cybersecurity assistance is a step down the path that Wortzel and McConnell espouse.

Though individuals with intimate knowledge of cybersecurity, including McConnell and Wortzel, have voiced their support for the NSA’s role as the lead government agency for cybersecurity, there is considerable opposition to this view. The NSA is often characterized as a “spy agency.”²⁰⁶ A blog post responding to Mike McConnell’s *Washington Post* article²⁰⁷ described the NSA as “the ultra-secretive government spy agency that is responsible for both listening in on other countries and for defending *classified* government computer systems.”²⁰⁸ This critique supports the NSA’s involvement in helping private companies enhance their security systems, as some companies already do, and as

²⁰² *Wortzel Testimony*, *supra* note 200.

²⁰³ *Id.*

²⁰⁴ Mike McConnell, *We’re Losing the Cyber-War, Here’s the Strategy to Win It*, WASH. POST, Feb. 28, 2010, at B01, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493_pf.html.

²⁰⁵ *Id.*

²⁰⁶ Ryan Singel, *Cyberwar Hype Intended to Destroy the Open Internet*, THREAT LEVEL BLOG, WIRED (Mar. 1, 2010, 6:56 P.M.), <http://www.wired.com/threatlevel/2010/03/cyber-war-hype>; see also *Cybersecurity Is Not Your Gig, NSA!*, *infra* note 223.

²⁰⁷ See McConnell, *supra* note 204.

²⁰⁸ Singel, *supra* note 206.

2010]

CYBERSECURITY AT INTERNET SPEED

209

McConnell has advocated.²⁰⁹ Opponents of the NSA's involvement in protecting private corporations believe that these companies "have no business letting the NSA into their networks or giving the NSA information that they won't share with the American people"²¹⁰ and appear to draw an arbitrary line at large companies like Google. This critique denies that a "cyberwar" exists, and that therefore, the involvement of the NSA, the "spy agency," will not help to protect against cyberwar attackers; rather, it will only threaten the openness of the Internet. This view suggests that its proponents are afraid of the strength and power of large corporations and therefore choose to remain ignorant of legitimate cyber threats.

2. Information Sharing: Problems, Questions, and Concerns

Google's announcement that it was targeted in a cyber attack was incredibly significant due to its size and high profile. As discussed above, however, Google and the NSA disclosed little about the details of their subsequent partnership. According to both the NIPP and a report published by the Government Accountability Office ("GAO") in March 2009, information sharing is an integral part of the strategy to secure cyberspace.²¹¹ The term "information" includes public awareness of the national security risks associated with cyberspace as well as the knowledge of intrusions that are increasingly likely under the current security regime.²¹² The GAO report recommended an aggressive awareness campaign to increase the knowledge of both leaders and the general public that the nation is regularly subjected to cyberattacks.²¹³

The GAO report also recommended White House accountability and responsibility for the leadership and oversight

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ See 2006 NIPP, *supra* note 20, at 14; see also U.S. GOV'T ACCOUNTABILITY OFFICE, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE (Mar. 10, 2009) [hereinafter GAO], available at <http://www.gao.gov/new.items/d09432t.pdf>.

²¹² GAO, *supra* note 211, at 9.

²¹³ *Id.*

of national cybersecurity policy.²¹⁴ While the Obama administration has taken steps toward improvements in cybersecurity,²¹⁵ the White House is conspicuously absent from the Google-NSA alliance, and White House leadership is never mentioned in the text of the National Infrastructure Protection Plan. The NIPP dictates the appointment of a Sector-Specific Agency for each CIKR sector, with DHS at the forefront of cyber efforts, and ongoing information sharing efforts between public and private entities within each sector.²¹⁶ By contrast, the GAO report argues that the White House, rather than a government agency, must assume a leadership role in order for consciousness to be raised regarding national cybersecurity concerns, both “to be successful and to send the message to the nation and cyber critical infrastructure owners that cybersecurity is a priority.”²¹⁷ The report states that without accountability, information sharing can be jeopardized because there is no authority implementing and employing incentives to encourage action, a large part of which is information sharing.²¹⁸

The discussion of Google’s Privacy Policy in Part I.B of this Note raises additional questions about information sharing. The information provided to Google by a given user is supposedly only used “for the purposes described in [its] Privacy Policy and/or the supplementary privacy policy notices for specific services[,]”²¹⁹ with several additional purposes listed. One such supplement, “[p]rotecting the rights or property of Google or our users,”²²⁰ fits squarely in the context of the China cyberattacks. Google’s intellectual property was stolen as a consequence of these attacks,²²¹ and it follows that the “rights or property” addition to

²¹⁴ GAO, *supra* note 211, at 8.

²¹⁵ See, e.g., CYBERSPACE POLICY REVIEW, *supra* note 20; Remarks by the President, *supra* note 20; see also GOV’T ACCOUNTABILITY OFFICE, CYBERSECURITY: PROGRESS MADE BUT CHALLENGES REMAIN IN DEFINING AND COORDINATING THE COMPREHENSIVE NATIONAL INITIATIVE (Mar. 2010), available at <http://www.gao.gov/new.items/d10338.pdf>.

²¹⁶ See *supra* Part I.A.

²¹⁷ GAO, *supra* note 211, at 8.

²¹⁸ *Id.*

²¹⁹ Google Privacy Policy, *supra* note 94.

²²⁰ *Id.*

²²¹ Drummond, *A New Approach to China*, *supra* note 144.

2010]

CYBERSECURITY AT INTERNET SPEED

211

the privacy policy would allow the personal information of Google users to be turned over to the NSA in conjunction with any investigation conducted by the alliance.

Though Google says it will ask for consent before sharing personal information with other companies or individuals outside of Google, one of the specifically enumerated circumstances for sharing personal information is applicable in large part to the Google-NSA alliance. Google will share personal information when there is

a good faith belief that access, use, preservation, or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or *enforceable government request*, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security, or technical issues, or (d) protect against harm to the rights, property, or safety of Google, its users or the public as required or permitted by law.²²²

The language “enforceable government request” suggests that if the NSA were to request personal information about Google users as a part of its investigation into the cyberattacks, Google could, and very well might, provide it. Organizations such as the American Civil Liberties Union and the Electronic Privacy Information Center vigorously criticize the NSA’s involvement in cybersecurity, especially in the context of the alliance with Google because so few details have been publicized.²²³ However, this type

²²² *Google Privacy Policy*, *supra* note 94 (emphasis added).

²²³ See, e.g., *Cybersecurity Is Not Your Gig, NSA!*, BLOG OF RIGHTS: OFFICIAL BLOG OF THE AM. CIVIL LIBERTIES UNION (Feb. 9, 2010), <http://www.aclu.org/blog/national-security-technology-and-liberty/cybersecurity-not-your-gig-nsa>; *EPIC Seeks Records on Google-NSA Relationship*, ELEC. PRIVACY INFO. CTR. (Feb. 4, 2010), <http://epic.org/2010/02/epic-seeks-records-on-google-n.html>; *EPIC Sues NSA to Force Disclosure of Cyber Security Authority*, ELEC. PRIVACY INFO. CTR. (Feb. 4, 2010), <http://epic.org/2010/02/epic-sues-nsa-to-force-disclos.html>; *U.S. Security Agencies Begging for a Cybersecurity “Cold War,”* BLOG OF RIGHTS: OFFICIAL BLOG OF THE AM. CIVIL LIBERTIES UNION (Mar. 3, 2010), <http://www.aclu.org/blog/national-security-technology-and-liberty/us-security-agencies-begging-cybersecurity-cold-war>.

of criticism would exist regardless of the particular government agency leading national cyberspace protection efforts and the fact still remains that cyberattacks are continually being launched against the United States.

3. The Alliance Is Answering a Call for Change

The history of cybersecurity policy in the United States as discussed in Part I.A of this Note demonstrates the nation's increasing dependence on cyber-based systems in many of its CIKR sectors. The government remains aware that "traditional telecommunications and Internet networks continue to converge, and other infrastructure sectors are adopting the Internet as a primary means of interconnectivity."²²⁴ Many of the most recent initiatives call for a change in leadership structure on the government side of the public-private partnership, and the Google-NSA alliance is accomplishing this goal with the NSA's assumption of leadership as the public sector partner in the collaboration.

While a large portion of the most recent cybersecurity initiative, the Cyberspace Policy Review released in late 2009, remained consistent with previous government cybersecurity policies, one recommendation was a relatively new and notable change: a call for White House leadership.²²⁵ Like the NSA's leadership in the Google-NSA alliance, this recommendation marks a significant departure from previous initiatives, which generally called for Sector-Specific Agencies to assume leadership roles for CIKR protection of individual sectors.²²⁶ The Cyberspace Policy Review goes so far as to say that "[t]he status quo is no longer acceptable . . . federal leadership and accountability for cybersecurity should be strengthened . . . [by] clarifying the cybersecurity-related roles and responsibilities of federal departments and agencies."²²⁷ Such statements could be considered an admission that the previous initiatives have been

²²⁴ CYBERSPACE POLICY REVIEW, *supra* note 20, at iii.

²²⁵ *Id.* at v.

²²⁶ See, e.g., 2006 NIPP, *supra* note 20; PDD 63, *supra* note 10; HSPD-7, *supra* note 20.

²²⁷ CYBERSPACE POLICY REVIEW, *supra* note 20, at iii.

unsuccessful. At a minimum, this proclamation calls for changes in cybersecurity policy, and the Google-NSA alliance might well be a change in the right direction. Despite the few available details about the alliance, the NSA's significant role in the collaboration marks a shift from the established cybersecurity functions of federal agencies.

Related to this change is the fact that the National Infrastructure Protection Plan tasks the Department of Homeland Security with the primary responsibility for cybersecurity policy, as evidenced by its designation as the Sector-Specific Agency for the Telecommunications and Information Technology sectors.²²⁸ As indicated in the Cyberspace Policy Review, however, there is a cyber dimension across CIKR sectors due to increased use of the Internet as a primary source of interconnectivity.²²⁹ The call for a change in cybersecurity policy leadership is a response to the perceived ineffectiveness under the leadership of DHS and the increased convergence of sectors around the cyber dimension. In May 2009, President Obama stated that for cybersecurity purposes, "federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should—with each other or with the private sector."²³⁰

4. The Government Is Not Keeping Pace With Its Plan

The Cyberspace Policy Review issued by the White House outlined a timeline for actions to be taken in the near and long term to improve cybersecurity policy.²³¹ Melissa Hathaway, the former Senior Director for Cyberspace, served under both the Bush and Obama administrations and publicly expressed concern prior to the Google attacks that the government was not meeting the challenges identified in the Cyberspace Policy Review.²³² The country has

²²⁸ See 2006 NIPP, *supra* note 20, at 3.

²²⁹ See CYBERSPACE POLICY REVIEW, *supra* note 20, at iii.

²³⁰ Remarks by the President, *supra* note 20.

²³¹ See CYBERSPACE POLICY REVIEW, *supra* note 20, at 37–38.

²³² Melissa Hathaway, *Government Must Keep Pace with Cybersecurity Threats*, INFO. SEC. MAG. (Oct. 2009), available at http://searchsecurity.techtarget.com/magazine/Feature/0,296894,sid14_gci1370150_mem1,00.html. Among Ms. Hathaway's accomplishments are the following: leading the 60-day interagency review of cybersecurity policies and programs across the federal government, overseeing the

increasingly relied on technology in day-to-day activities, and Hathaway writes that the United States has “not invested in the resilience necessary to assure our businesses can operate in a degraded environment.”²³³ Reliance on remote access and the reduction in costs and manpower needs as a result of networked control systems have led to weaknesses that opponents can exploit.²³⁴ Accordingly, Hathaway states that the need for increased cybersecurity has not been adequately addressed and that any government response should be “focused, aggressive, and well-resourced.”²³⁵

Hathaway’s article also suggests that collaborative efforts between various agencies should “foster innovation and enable our information and communications infrastructure to fuel the nation’s economic growth.”²³⁶ While she applauds some recent efforts as “first steps toward making real and lasting progress” in securing cyberspace, bold steps and increased information sharing are still required to protect the nation’s networks.²³⁷ Even Mike McConnell, in his strongly worded support of the NSA’s leadership wrote that “[t]he time to start [protecting cyberspace] was yesterday.”²³⁸

B. The Google-NSA Alliance Reflects the Effectiveness of Current Government Cybersecurity Policy

Several key elements of the Google-NSA alliance align with existing government initiatives concerning cybersecurity. Specifically, despite the dearth of publicized details about the alliance, it fits within the framework of a public-private

development of the *Cyberspace Policy Review*, helping build the Comprehensive National Cybersecurity Initiative (“CNCI”) under the Bush administration, leading development of a cross-agency budget submission to support CNCI, establishing relationships in Congress to gain bipartisan support for cybersecurity initiatives, testifying and briefing with legislators over 150 times, and consulting with DoD and the intelligence community in her capacity as a former principal at Booz Allen Hamilton. *Id.*

²³³ *Id.*

²³⁴ See *id.*

²³⁵ *Id.*

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ McConnell, *supra* note 204.

partnership, which the government has identified as the key to CIKR protection. The alliance is voluntary, as Google approached the NSA, not the other way around. Finally, the alliance represents a step towards improving cybersecurity practices by addressing the existing lack of awareness as articulated in the National Strategy to Secure Cyberspace. The combined power and resources of the two organizations could result in new standards for cybersecurity protection and will surely increase public awareness of the cyber threat.

1. The Alliance Can Be Characterized as a Public-Private Partnership

Since the issuance of President Clinton's PDD-63 directive in 1998, technology has been considered part of the critical infrastructure of the United States, and accordingly is best protected through a collaborative relationship between the public and private sectors.²³⁹ Government initiatives between 1998 and the present day cite the public-private partnership as the key to securing the nation's critical infrastructure.²⁴⁰ The National Infrastructure Protection Plan provides that Sector-Specific Agencies are "responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector."²⁴¹ In the context of the alliance, the NSA fills the role of a Sector-Specific agency for technology and cyber systems in collaborating with a private sector partner, Google.²⁴²

According to the articles written about the alliance, Google's motive for soliciting assistance from the NSA was to assess risk and help defend against future cyberattacks.²⁴³ Google's prominent role in the cyber sector could result in the sharing of

²³⁹ PDD 63, *supra* note 10.

²⁴⁰ See *supra* Part I.A.

²⁴¹ 2006 NIPP, *supra* note 20, at 19.

²⁴² The NIPP designates DHS, not the NSA, as the lead agency for the technology sector. See *supra* Part II.B.2.

²⁴³ See, e.g., Nakashima, *supra* note 162 (stating that the partnership's objective was to better defend Google).

security-related information within the sector, which will be discussed later in this Note.²⁴⁴

2. The Alliance Was Formed Voluntarily

As reported in both *The New York Times* and the *Washington Post*, Google approached the NSA for assistance, not the other way around. The National Infrastructure Protection Plan specifically states that “[p]rivate sector owners and operators are responsible for taking action to support risk management planning and investments in security . . .”²⁴⁵ The level of investment in security depends on a risk versus consequence analysis.²⁴⁶ First, private sector enterprises consider what is known about the risk environment,²⁴⁷ and in the cyber world, the answer is usually very little due to the dynamic nature of the cyber risk environment.²⁴⁸ The federal government, however, can help inform critical security investment decisions and operational planning,²⁴⁹ which is exactly the position that the NSA has taken with Google.

Private companies also consider what is economically viable in a competitive marketplace or an environment of limited resources.²⁵⁰ Owners and operators in the private sector often “rely on government entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise’s capability to protect itself or mitigate risk.”²⁵¹ Google’s decision to pull out of China is a clear indication that the threat was substantial, and accordingly it has enlisted the NSA because the China threat was significant enough to lead Google to at least question its capability to protect itself.

²⁴⁴ See discussion *infra* Part II.B.3.

²⁴⁵ 2006 NIPP, *supra* note 20, at 26.

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ See Cybersecurity, Innovation and the Internet Economy, 75 Fed. Reg. 44216 (July 28, 2010).

²⁴⁹ 2006 NIPP, *supra* note 20, at 26.

²⁵⁰ See *id.*

²⁵¹ *Id.*

3. The Alliance Represents a Step Toward Addressing Cyber Vulnerabilities and Best Practices

The pairing of the NSA and Google aligns with the government's goal of implementing protection programs across the various CIKR sectors.²⁵² The NIPP states that “[t]he risk assessment and prioritization activities within each sector will help identify requirements for current protective programs and shortfalls for future efforts.”²⁵³ Even if the findings and solutions implemented as a result of the alliance are never released to the public, they can be shared within each individual sector as “best practices” and to improve protective actions, which “involve measures designed to prevent, deter and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation.”²⁵⁴

If no other details of the alliance are made available, the cyberattacks on Google and capabilities of the NSA, discussed in Part I, support the argument that Google approached the NSA to utilize its security expertise in furtherance of these and other goals. Publicizing the attacks is an admission of Google's vulnerabilities to attacks on its infrastructure, and by partnering with the NSA it wishes to minimize consequences for its users and work toward elimination of the threat.

The partnership was announced within a month after Google publicly announced that a cyberattack had occurred.²⁵⁵ This quick response is timely and efficient, and constitutes a measure to restore both the company's own confidence in its security measures and the trust and support of Google users worldwide. Regardless of the final outcome of the alliance, it addresses current cyber vulnerabilities, and could result in the application of a set of best practices to be shared within the cyber and technology sectors.

²⁵² See *id.* at 45–48.

²⁵³ *Id.* at 45.

²⁵⁴ *Id.*

²⁵⁵ The Google attacks were announced on January 12, 2010, and the *Washington Post* article appeared on February 4, 2010. See Drummond, *A New Approach to China*, *supra* note 144; Nakashima, *supra* note 162.

4. The Alliance Promotes Information Sharing Between the Public and Private Sectors

The interdependence between the public and private sectors is readily apparent in the technology sector and beyond. Much of the nation's critical infrastructure, including transportation systems, communication networks, and the national power grid, depends upon the ability of networks in both the public and private sectors to share information in cyberspace.²⁵⁶ The Google-NSA partnership can allow for the sharing of critical information to analyze the recent attack on Google without infringing privacy rights.²⁵⁷ The alliance is a real-world manifestation of a stated policy goal of the United States and could allow the country "to develop a unified and coordinated approach to defending our nation's assets."²⁵⁸ One proponent of this course of action believes that specifically, "[t]his alliance will help Google better defend its intellectual property critical to our nation's economy while providing the NSA key insight into the attack methods and motives of the attackers."²⁵⁹

Mike McConnell wrote in an article in the *Washington Post* that "an effective partnership with the private sector [must be formed] so information can move quickly back and forth from public to private and classified to unclassified—to protect the nation's critical infrastructure."²⁶⁰ While he acknowledges that arrangements like this alliance "will muddy the waters between the traditional roles of the government and the private sector," McConnell states that the Google-NSA partnership "point[s] to the kind of joint efforts—and shared challenges" that are likely to be seen in the future.²⁶¹

²⁵⁶ *Google, The NSA, and the Increasing Interdependence Between the Public and Private Sectors*, FED. NEWS RADIO, Feb. 18, 2010, <http://stage-v4.federalnewsradio.com/?sid=1891928&nid=293>.

²⁵⁷ *Id.*

²⁵⁸ *Id.*

²⁵⁹ *See id.*

²⁶⁰ McConnell, *supra* note 204.

²⁶¹ *Id.*

III. PROBLEMS ACROSS SECTORS FURTHER SUGGEST THAT CURRENT CYBERSECURITY POLICY NEEDS IMPROVEMENT

The public-private partnership has been a cornerstone of critical infrastructure protection for over a decade. In its basic structure, the Google-NSA alliance fits within the framework of the public-private partnership: a government entity and a private corporation collaborating to better protect cyberspace. The alliance preserves several of the foundation principles of cyber policy from 1998 to the present, most notably the basic structure of the public-private partnership. In addition, the initiative taken by Google, the private sector counterpart, to work with the NSA as a government partner comports with the NIPP, which is demonstrative of the effectiveness of the policy. Regardless of whether the alliance ultimately proves successful, it addresses current cyber vulnerabilities, and the relative success or failure of this partnership could help in shaping best practices to be shared within the cyber and technology sectors. Finally, endorsements from two individuals (Wortzel and McConnell) with significant knowledge and expertise in cybersecurity and the current initiatives, can be considered a strong indication that the alliance is not a significant departure from current policies.

Though the Google-NSA alliance retains some important elements of the current cybersecurity posture, its differences from the policies in force are much more significant. First, while DHS rather than the NSA has traditionally served as the lead government agency in critical infrastructure protection within the technology sector, the NSA functions as the de facto lead government agency in the Google-NSA alliance. The alliance, then, allows the NSA to fill a considerably broader role than previously provided for it in the NIPP and significantly departs from the current policies.

Cyber systems also transcend individual CIKR sectors due to their broad reach, as indicated by the support of the NSA's leadership by several individuals with highly specialized knowledge of cyberspace and national security. Proponents of this course of action urge that the NSA, rather than DHS, assume a leadership role in cyberspace protection because protective efforts would not be confined to a given sector. However, as presently

drafted, existing policies do not contemplate such a role for the NSA. Moreover, substituting the NSA for DHS would not significantly disturb the framework of the public-private partnership; it simply substitutes one government actor for another. However, because the current regime tasks only DHS with cyberspace protection, Google's choice to partner with the NSA represents a departure from the type of public-private partnership contemplated by the NIPP and other initiatives.

In publicizing news about the China cyberattacks, Google remained silent about the details of its subsequent partnership with the NSA, refusing even to confirm or deny the news reports. Merely publicizing information about the attack is insufficient to satisfy the recommendations of the GAO report and the NIPP to drastically raise the level of national awareness about cyberspace protection. An increase in information sharing between public and private entities cannot reasonably be anticipated without national awareness; there is therefore little room for improvement of the existing cybersecurity measures without it. The alliance also does not comport with either the GAO or the NIPP regarding national awareness of cyber protection, which is indicative of inconsistencies in cybersecurity policies. These inconsistencies in turn suggest that the current initiatives are largely ineffective and that the Google-NSA alliance is a positive development in cybersecurity.

The most recent initiatives also appeal for a change in government leadership structure, and the Google-NSA alliance is accomplishing this goal with the NSA's assumption of leadership as the public sector partner in the collaboration. Finally, the government has fallen behind in its implementation: current policies make broad recommendations about how to proceed with cyberspace protection, but little improvement has been seen to date. The alliance represents a significant step away from the present initiatives as a response to this lack of progress.

Taken as a whole, these departures from current cybersecurity initiatives indicate that the existing regime is glaringly defective. The defects of the current posture and policies are perhaps best illustrated by another established public-private partnership, also falling squarely within the overarching domain of cyberspace: the

Defense Industrial Base (“DIB”), governed by the Department of Defense as its Sector-Specific Agency pursuant to the National Infrastructure Protection Plan.²⁶² “The DIB is DoD, the U.S. government, and the private sector worldwide industrial complex with capabilities to perform research and development (“R&D”), design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.”²⁶³ It includes many thousands of foreign and domestic entities, as well as their subcontractors, who perform work for the Department of Defense and other federal departments and agencies.²⁶⁴ The Defense Industrial Base provides defense-related products and services used to “equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide,”²⁶⁵ which includes the domain of cyberspace. Only a small percentage of Defense Industrial Base facilities are actually owned by the Department of Defense, so the efforts described in the Defense Industrial Base Sector-Specific Plan (“DIB SSP”) largely “focus on DoD and government actions to support private owner/operator efforts at DIB facilities determined to be critical to national security.”²⁶⁶

The DIB SSP divides the sector into segments, sub-segments, and commodities.²⁶⁷ While many of the Defense Industrial Base segments are irrelevant for purposes of this Note, the information technology segments, which encompass the sub-segments of

²⁶² U.S. DEP’T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN 3 (2007) [hereinafter *DIB SSP*], available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf>.

²⁶³ *Id.* at 4.

²⁶⁴ *Id.* at 5.

²⁶⁵ *Id.*

²⁶⁶ *Id.*; cf. DEP’T OF DEF., DEPARTMENT OF DEFENSE DIRECTIVE NUMBER 3020.40 (Aug. 19, 2005), available at http://www.fas.org/irp/doddir/dod/d3020_40.pdf. The Directive updates, renames, and reissues the Defense Critical Infrastructure Program (DCIP), “which addresses DIB assets owned by the private sector and DOD-owned elements of the DIB. Thus, the DIB plan purports to focus on the privately owned and operated efforts at DIB facilities rather than on the small fraction of DIB facilities owned by the DOD.” Lieutenant Colonel Todd A. Brown, *Sovereignty in Cyberspace: Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 226–27 (2009).

²⁶⁷ See *DIB SSP*, *supra* note 262, at 5–6.

“command control, computers, and intelligence [and] information security” within the Defense Industrial Base, link the information technology sector (governed by the Department of Homeland Security, pursuant to the National Infrastructure Protection Plan) to the defense sector.²⁶⁸ Cyberspace extends across critical infrastructure sectors,²⁶⁹ and the unifying factor of information technology creates an especially strong parallel between these two sectors. To facilitate information sharing, the DIB SSP identifies security partners within the federal government and Department of Defense itself, within the private sector, and on a state, local, and international scale.²⁷⁰

Lieutenant Colonel Todd A. Brown²⁷¹ argues that the DIB SSP is deficient in identifying the specific efforts the Department of Defense will take to coordinate CIKR protection within the private sector; rather, he claims that the plan “restates the edits of HSPD-7 and the NIPP” and points out that the “D[o]D will work with the DHS to identify overlaps and gaps in responsibility with other sector-specific agencies with regard to DIB assets that belong to other sectors.”²⁷² Brown believes that the plan is “particularly inadequate [in] its reference to cyber security risks,”²⁷³ and the plan itself actually maintains that “[w]hile cyber security is an issue that could affect any facility, DoD does not perform network- or system-level assessments.”²⁷⁴ Rather, the plan states that “DIB assets are primarily owned by the private sector; and that (1) there are no regulatory requirements for conducting formal risk assessments, (2) large companies conduct their own risk assessments as part of prudent business practices, and (3) the

²⁶⁸ *Id.* at 5.

²⁶⁹ See *supra* Part II.A.3.

²⁷⁰ See *DIB SSP*, *supra* note 262, at 6–10.

²⁷¹ Brown currently serves as the Judge Advocate for the 187th Fighter Wing of the Alabama Air National Guard. See *187th Fighter Wing, Resources*, ALA. AIR NAT'L GUARD, <http://www.187fw.ang.af.mil/resources/index.asp> (last visited Aug. 10, 2010).

²⁷² Brown, *supra* note 266, at 227.

²⁷³ *Id.* Indeed, the government has begun to recognize its deficiencies in approaching sector-specific planning against cyber threats. See GOV'T ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: CURRENT CYBER SECTOR-SPECIFIC PLANNING APPROACH NEEDS REASSESSMENT (Sept. 2009), available at <http://www.gao.gov/new.items/d09969.pdf>.

²⁷⁴ *DIB SSP*, *supra* note 262, at 17.

D[o]D aims to ensure awareness and risk management best practices throughout the DIB.”²⁷⁵ The National Infrastructure Protection Plan emphasizes a “single national effort” for integration of the United States’s CIKR protection initiatives,²⁷⁶ and Brown expresses concern that small members of the Defense Industrial Base in the private sector are being overlooked, because they may not have the resources to conduct risk assessments on the same scale as large companies, and asks how the Department of Defense “aim[s] to ensure awareness across the entire sector.”²⁷⁷

Google, a veritable giant in the realm of technology and cyberspace, is a large private company with significant resources available to assess the risk of cyber threats it may confront.²⁷⁸ As indicated by the recent partnership with the NSA, Google has enlisted help from the government in analyzing the cyber risks it has already faced and will continue to combat, presumably because its own cybersecurity resources have proven insufficient. If the resources of large private companies in the Telecommunications/Information Technology sectors are proving to be inadequate, it is unreasonable to assume that smaller private entities within the sector have the capabilities to defend against cyber threats. Applying Brown’s perspective on the Defense Industrial Base to this sector, however, exposes a strong parallel between the two sectors: small-scale members of private industry across CIKR sectors face unique challenges in forming public-private partnerships. These obstacles are twofold: smaller private entities do not have the resources of a giant like Google to assess cyber risks on their own, and may not be aware of the opportunities for information sharing available to them under the National Infrastructure Protection Plan. Thus, both the Defense Industrial Base and the technology sector have considerable gaps to fill in cybersecurity protection as articulated by the National Infrastructure Protection Plan, suggesting that the current policies are ineffective.

²⁷⁵ Brown, *supra* note 266, at 227–28.

²⁷⁶ 2006 NIPP, *supra* note 20, at i.

²⁷⁷ Brown, *supra* note 266, at 228.

²⁷⁸ See *supra* Part II.

Brown also argues that the DIB SSP is noncompliant “with the HSPD-7 directive that the tasked departments share information about cyber threats.”²⁷⁹ The National Infrastructure Protection Plan recommends that information sharing between the public and private sectors be conducted using a networked approach²⁸⁰ with significant reliance on critical infrastructure information provided by the private sector.²⁸¹ However, the DIB SSP does not discuss coordination of information sharing; rather, it states that the Department of Defense “relies on private sector organizations to exchange information regarding DIB infrastructure.”²⁸² Brown asserts that responsibility for these information-sharing efforts is being relegated back to the Department of Homeland Security, while the Department of Defense seems to take on a supporting role in “efforts to address cyber incidents, conduct vulnerability assessments, develop risk management strategies, and facilitate information sharing.”²⁸³ The DIB SSP lists a number of federal agency partners in its CIKR protection within the sector, including the Department of Homeland Security: the Office of Infrastructure Protection (“OIP”) and the Office of Cyber Security and Telecommunications (“CST”) are jointly “responsible for deterring, preventing, and defeating cyber incidents across all CI[JKR] sectors.”²⁸⁴ As discussed in Part II.A.3, the most recent policy initiatives have called for a change in cybersecurity policy leadership. Thus, the argument that the Google-NSA alliance is a distinct departure from current policies due to inefficiencies is further strengthened by the analogous difficulties in information sharing within the Defense Industrial Base, a related CIKR sector.

Perhaps the most salient point of Brown’s analysis is that the emphasis on voluntary participation on the part of the private sector is the greatest challenge in successful information sharing.²⁸⁵ The sensitive nature of such information, be it relevant to business or security, renders its safekeeping critical because

²⁷⁹ Brown, *supra* note 266, at 228.

²⁸⁰ See 2006 NIPP, *supra* note 20, at 57–66.

²⁸¹ Brown, *supra* note 266, at 228.

²⁸² *Id.* (quoting DIB SSP, *supra* note 262, at 7).

²⁸³ Brown, *supra* note 266, at 228.

²⁸⁴ DIP SSP, *supra* note 262, at 8.

²⁸⁵ Brown, *supra* note 266, at 228–29.

unauthorized disclosure or access could result in “serious damage to private industry, the economy, public safety, or public security.”²⁸⁶ As such, the information sharing problems and concerns discussed in Part II.A.2 of this Note are pervasive across sectors,²⁸⁷ further reinforcing the argument that current government cybersecurity policies are largely ineffective. It follows that the Google-NSA alliance represents a departure from these strategies pursuant to the most recent initiatives taken regarding cybersecurity policy, and proposes a unique solution to the problems the United States faces in the cybersecurity arena.

Whether or not the Google-NSA alliance is ultimately successful in filling the gaps left by current cybersecurity policy, it should be viewed as a step toward improvement. Members of both the public and private sectors have expressed concern about cybersecurity in the United States,²⁸⁸ and this unlikely pairing represents a unified front to address a common concern. The framework of the alliance has incorporated the hallmarks of the current policy initiatives, most significantly the public-private partnership, which should be satisfactory to those supporters of the present policy framework. While many outspoken critics reject the notion of “cyberwar” generally and the security concerns that logically follow, some even saying that cyberwar does not exist,²⁸⁹

²⁸⁶ *Id.* at 229.

²⁸⁷ See Gov’t ACCOUNTABILITY OFFICE, INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE: OVERARCHING GUIDANCE IS NEEDED TO ADVANCE INFORMATION SHARING (Mar. 17, 2010), available at <http://www.gao.gov/new.items/d10500t.pdf>.

²⁸⁸ See Part I.A.3, for a discussion of government initiatives regarding cybersecurity policy. See also Grant Gross, *HP Lawyer: Tech Industry Needs to Focus on Privacy*, COMPUTER WORLD (June 8, 2010, 3:38 PM), http://www.computerworld.com/s/article/9177838/HP_lawyer_Tech_industry_needs_to_focus_on_privacy (discussing Holston’s remarks during the Brookings forum); *Technology and Trust: Privacy and Security Concerns Create Challenges and Opportunities for Innovation*, HEWLETT-PACKARD (July 5, 2010), http://hpnw.corp.hp.com/news/10q3/100705ex_str.htm (discussing the participation of Hewlett-Packard General Counsel Michael Holston in a forum hosted by the Brookings Institute to discuss improving science and technology innovation and investment in America. Holston emphasized that privacy and cybersecurity are chief among the issues faced by technology companies and governmental regulators.).

²⁸⁹ See, e.g., Bruce Schneier, *Threat of ‘Cyberwar’ Has Been Hugely Hyped*, CNN, July 7, 2010, <http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/#fbid=twl0xbGeedy&wom=false>; Jeffrey Carr, *The Top Five Cyber Fallacies*, THE FIREWALL BLOG, FORBES (Mar. 29, 2010, 6:00 AM), <http://blogs.forbes.com/firewall/2010/>

the fact remains that Google, an Internet giant in every sense of the word, was subjected to cyberattacks.²⁹⁰ It subsequently admitted its security vulnerabilities and strongly suggested that its users take precautions when using the Internet. Though this statement is far from an admission of the existence of “cyberwar,” it is conclusive proof of a significant threat. Current policies are simply not enough to combat the severity of the threats posed by cyberspace. Though the security measures that have been taken form a solid foundation, the existing cyberspace protection programs are simply insufficient. The Google-NSA alliance has reformulated the touchstones of the early and present cybersecurity efforts to increase voluntary information sharing and best practices between the public and private sectors. Initiatives such as the Google-NSA alliance must be supported by the public to prevent further cyberattacks and increase the security of the nation’s cyber systems.

CONCLUSION

The Google-NSA alliance is unprecedented, regardless of whether it actually demonstrates a departure from the nation’s current cybersecurity policies. In comparing the Defense Industrial Base and the Telecommunications and Information Technology sectors, a larger problem emerges: in practice, current cyberspace protection programs simply do not have the broad reach across individual sectors that PDD-63 and its progeny intended. Cybersecurity is a necessary component of CIKR protection across the nation’s infrastructure, and the most recent cybersecurity policies essentially acknowledge the shortcomings of the present initiatives.²⁹¹

If the Google-NSA alliance proves to be a solution to the deficiencies of present cybersecurity policy, it would not be

03/29/the-top-five-cyber-fallacies; Richard Stiennon, *The Ten-Year-Old “Cyberwar” Debate Continues*, THE FIREWALL BLOG, FORBES (June 16, 2010, 9:59 AM) <http://blogs.forbes.com/firewall/2010/06/16/the-ten-year-old-cyberwar-debate-continues>.

²⁹⁰ See *supra* Part I.B.2.

²⁹¹ See CYBERSPACE POLICY REVIEW, *supra* note 20, at iii; Remarks by the President, *supra* note 20.

2010]

CYBERSECURITY AT INTERNET SPEED

227

infallible because questions of privacy, international implications, and information sharing and security remain. The Google cyberattacks that prompted the alliance resulted in theft of intellectual property, which can be characterized as “the heart and core value of companies worldwide.”²⁹² A global company’s intellectual property includes “trade secrets, proprietary formulas, copyrights, trademarks, and source code . . .”²⁹³ While privacy concerns about individual user data have a strong foundation, this Note proposes that even the strongest privacy advocate consider the large-scale implications resulting from corporate intellectual property theft. If a future cyberattack were to successfully obtain additional intellectual property belonging to Google, the security of Google users’ private information would be jeopardized. Cyberspace, by definition a difficult area to defend, remains largely unprotected, despite a decade’s worth of security initiatives. All users of the Internet should be supportive of the fledgling partnership between private industry and the public sector as they work towards the strongest possible security solution to secure cyberspace for the benefit of all Americans.

²⁹² MCAFEE LABS AND MCAFEE FOUNDSTONE PROF’L SERVS., PROTECTING YOUR CRITICAL ASSETS: LESSONS LEARNED FROM “OPERATION AURORA” 4, *available at* http://img.en25.com/Web/McAfee/NA_AURORA_MCAFEE_WP.pdf (last visited Sept. 16, 2010).

²⁹³ *Id.*